

# Terms and Conditions for E-Banking

## 1. E-Banking Services

- 1.1. The services offered by Bank Cler AG (hereinafter referred to as the "Bank") in E-Banking are described in the "Information on E-Banking". This forms an integral part of these terms and conditions. The "Information on E-Banking" can be accessed on the bank's website on the appropriate login page for E-Banking. The Bank reserves the right to amend these at any time.
- 1.2. Payment and stock exchange orders cannot be performed round the clock. Transaction times are given in the "Information on E-Banking".
- 1.3. The data exchange provided for in these terms and conditions relates to banking business which is based on separate agreements or terms and conditions of business. The following provisions take precedence over any differing terms and conditions in the said agreements or terms of business in the terms of reference of the services via E-Banking requested by the customer.
- 1.4. With use of the service "E-Documents," bank documents for bank/custody accounts are delivered to the customer and/or the user electronically via E-Banking. Existing mailing or archiving instructions are superseded, whereby, for example, bank/custody account statements, notices from the payment transactions, stock exchange trading invoices, and other notices/communications (hereinafter referred to as bank documents) are made available only electronically instead of in paper form within the scope of E-Banking to the person receiving the "E-Document" service. Final account settlement statements and tax certificates will continue to be issued by post. **The Bank's obligations of reporting and accountability to the customer are thereby fulfilled.**

## 2. User/login process/means of identification

- 2.1. Access to E-Banking is received by users who authenticate themselves by input of the means of identification as a part of the selected login process valid for these services. Users are defined as those persons authorized by the customer for use of E-Banking in the E-Banking agreement (i.e., the customer and/or authorized persons/users).
- 2.2. Required as means of identification for the use of E-Banking are:
  - a) the identification number provided to the user by the Bank;
  - and
  - b) the personal, freely selected password of the user;
  - and

c) an additional single-use code, which is sent contemporaneously in accordance with the relevant login process selected by the user, and after entering the valid identification number and the valid password must be entered or confirmed. The requirement of entering an additional code can be dispensed with according to the login process selected, for example, the use of a software certificate (SoftCert).

The individual login process made available by the Bank can also be amended according to the changed state of technology over the course of time and it will be described on the Bank's website and, if applicable, in the specific product or other documentation.

The Bank reserves the right to cancel existing login processes and introduce new ones, which can supplement or delete those described above.

- 2.3. Whosoever authorizes himself as per Number 2.2 (self-identification) applies as the authorized person vis-à-vis the Bank for use of E-Banking services as well as other electronic channels of the Bank, access to which requires relevant login.

The Bank may accordingly allow him within the scope and extent of the services and type of authorization selected in the E-Banking agreement by the customer, regardless of its legal relationship to the customer, unless they are identical, and irrespective of entries in the Commercial Register, publications or rules in the signature documents, as well as without further examination of their authorization and irrespective of the legal relationship of the Bank to the customer, to make inquiries, dispositions, refer electronically to documents as well as allow them to use other functions in the electronic channels of the bank, which are enabled through access to E-Banking login. It is also entitled to accept orders and legally binding notifications from them and to execute these.

- 2.4. The Bank has the right at any time and without stating reasons to refuse the provision of E-Banking services and to require that the user prove his identity in another form (by signature or personal appearance).
- 2.5. The customer accepts without reservation all transactions posted within the scope of the agreed E-Banking services by the user under use of his means of identification. Likewise, all instructions,

orders and notifications which reach the Bank by this means are deemed to be given and authorized by the customer and electronically provided documents as rightfully retrieved from the authenticated user.

### 3. Duties of care of the customer/user

- 3.1 The user undertakes 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 If the user receives any activation and/or verification codes for E-Banking services, then he is obligated to perform the activation and/or verification without delay and according to the instructions provided.
- 3.3 The user undertakes to ensure that all identifying means of information are kept secret and protect them against improper use by unauthorized persons. In particular, the password must not be recorded or stored without protection on the end device (such as a computer, laptop, tablet, or mobile telephone) or otherwise recorded. Likewise, the identifying information must not be disclosed or otherwise made available to third parties. In particular, he acknowledges that the Bank will never request by email that he provide his means of identification for E-Banking in any data entry mask or to send it in any way to the bank or to any other recipient.
- 3.4 The customer bears the risks which arise from use (including misuse) of his means of identification or those of the authorized persons unless the Bank fails to act with normal business due care.

Should damage or other detriment occur, without the Bank or the customer or user violating its or his duty of care, the party in whose sphere of influence the cause of the damage or the damaging act lies shall also be liable. The bank assumes no liability for damage or other detriments from transmission errors, technical problems and illegal interference with the devices or software of the user.

- 3.5 If there is cause for suspicion that unauthorized third parties have gained knowledge of one or more means of identification of an authorized user, the user must change the relevant means of identification immediately. If this is not possible, he must immediately request that access to the relevant services be blocked, or block access to the services himself, by undertaking the appropriate steps on the relevant websites of the Bank or by proceeding in accordance with Number 5.1 of these conditions.

- 3.6 If there is cause for suspicion that unauthorized third parties have gained access to the end device of the user (for example, in the case of loss or theft of the end device), the user is also obligated to contact without delay the Bank's hotline service by telephone during the support times published on the websites of the Bank.
- 3.7 The user is required to examine all data entered by him for completeness and correctness. Responsibility concerning data communicated by the user remains with the customer.

### 4. Exclusion of liability of the Bank and its employees

- 4.1 The Bank accepts no guaranty for the completeness and correctness of data displayed by it in E-Banking. In particular, details of bank accounts and custody accounts (balances, statements, transactions, etc.) as well as generally accessible information, such as stock-exchange prices and currency rates, are deemed to be non-binding, unless they are explicitly designated as such. Authoritative are the details in the statements and documents of the bank, which were delivered to the customer in paper form or electronically.
- 4.2 The Bank does not arrange technical access to its services. This is the sole responsibility of the user. More particularly, they acknowledge that the Bank does not distribute the special software necessary for internet access and for the use of E-Banking nor does the Bank support the user in respect of software or hardware problems. The Bank accordingly accepts no guarantee for either the network operator (service provider) or for the necessary software.
- 4.3 Data transactions are conducted over public telecommunications networks not specially protected (telephone, Internet, etc.). The Bank excludes liability for losses arising from use of these networks. More particularly, the Bank accepts no liability for damage incurred by the customer/user as a consequence of communication faults, technical defects, interruptions in the telephone network or the internet, illegal tampering with network installations, overloading in the networks, wilful blocking of electronic access by third parties, breakdowns or other deficiencies on the part of the network operator.
- 4.4 In spite of all security measures, the Bank cannot accept any liability for the terminal unit of the user, as this is not possible from a technical standpoint (concerning risks cf. Number 8).
- 4.5 Furthermore, the Bank expressly excludes liability for software possibly recommended or supplied by it (for example, CD, download, or apps), as well as the consequences arising from and during transfer of the software via the Internet.

- 4.6 The Bank, on the application of the customary degree of care, accepts no liability for the consequences of faults and interruptions, more particularly in operating E-Banking (for example, caused by illegal access to the system).
- 4.7 The Bank reserves the right at any time to interrupt E-Banking for the protection of the customer/user on discovery of security risks, until their elimination. The Bank accepts no liability for any losses arising from such an interruption.
- 4.8 If orders are defectively or incorrectly not executed or not executed on time and damage is suffered, the Bank is liable at most for the loss of interest (does not apply to stock exchange orders).

### 5. Block

- 5.1 The customer can have his own access or that of users authorized by him to the E-Banking services blocked. Customers can also have the access of their users to E-Banking services blocked. Blocking can only be requested during the times stipulated in the "Information on E-Banking". The Bank can require additional confirmation of the block in writing. The user can also block access to the services in E-Banking himself at any time by entering an incorrect password or an incorrect additional code three times in a row if the login process used by him requires entering an additional code.
- 5.2 The Bank can require that the block be removed by him or another user only with written consent.
- 5.3 The Bank may likewise block access of the user to individual or all services at any time without stating reasons and without prior termination of the agreement if this in its own judgment shall appear to be indicated for practical reasons.

### 6. Power of attorney conditions

Entitlement of a user to the use of E-Banking services is valid until written revocation addressed to the Bank. The deletion or amendment of the power of attorney or subscription rights of the authorized persons pursuant to the signature documentation lodged with the bank or the deletion or amendment of the subscription rights of a user in the Commercial Register does not automatically bring about the revocation of their authorization for the use of E-Banking.

In the event of death and possible loss of legal capacity of the customer, the authorization granted does not automatically expire.

### 7. Financial assistant

- 7.1 The Bank makes a financial assistant available. This represents a service as a part of the Bank's E-Banking or of the Bank's electronic channels. The financial assistant supports the customer in the management of his personal finances.

- 7.2 In the framework of the financial assistant, account transactions and, insofar as explicit approval has been given for this as a part of E-Banking or the digital channels of the Bank, credit card transactions as well as data recorded from the customer will automatically be assigned to specified categories. The customer can always modify the assignment.
- 7.3 The confidentiality of the customer data is always safeguarded. No data which permit conclusions about a specific person, will be forwarded to third parties.
- 7.4 The customer can always deactivate the financial assistant in settings or can always revoke agreement to the inclusion of credit card data. At its own discretion, the Bank can temporarily or permanently discontinue the service.

### 8. Security in E-Banking

- 8.1 The customer acknowledges that the data are carried through a network accessible to all, the internet, which is accessible to everyone. The data are therefore regularly and without control transferred across borders. This also applies to data transfer where the sender and the recipient are both located in Switzerland. Although the individual data packages are transferred in an encoded form, the sender and the recipient on the other hand remain in each case unencoded and can also be read by third parties. Consequently, a conclusion may be drawn by a third party as to an existing banking relationship.
- 8.2 Special importance was attached to security in the development of E-Banking. A multi-step security system was developed for the security of the customer/user, which, among other things, has recourse to cryptographic procedures of a very high technical standard. In principle, because of the encoding, it is not possible for any unauthorized person to view confidential customer data. However, absolute security cannot be guaranteed either by the Bank or by the customer, even with security precautions meeting the highest, most technically advanced standards. The customer/user acknowledges in particular that his end device constitutes the weak link in accessing E-Banking. Regular updates to the software (e.g. the operating system) of the end device is the responsibility of the user.

8.3 The customer/user acknowledges in particular the following risks:

- Insufficient knowledge of the system and deficiencies in system precautions may facilitate unauthorized access (for example, insufficiently protected data storage on the hard disk, file transfers, screen radiation, etc.). It is incumbent upon the customer/user to inform himself of the necessary security precautions.
- Nobody can exclude the creation of a user profile by the user's internet provider; that is, this provider has the means to trace with whom the user is in contact.
- There is a permanent risk that a third party may gain access unnoticed to the user's end device during use of the internet (for example, through a Java or ActiveX application).
- There is a permanent risk that malware (such as computer viruses) may be spread in the user's end device by use of the internet, given the end device's contact with outside systems either through computer networks or other data carriers.
- It is expected that the user works only with software procured from a trustworthy source.
- Changes to the operating system of the user's end device (such as Jailbreak, Roots) can make it easier to gain unauthorized access.

## 9. Import and export restrictions

- 9.1 The customer/user of E-Banking acknowledges that in some circumstances he may be infringing the provisions of foreign law by using E-Banking outside Switzerland. It is the customer's/user's responsibility to seek information on this point. The Bank shall accept no liability in this respect.
- 9.2 The customer/user acknowledges that there may be import and export restrictions regarding encoded algorithms, which, if applicable, may be infringed when using E-Banking services in or from another country.

## 10. Customer data and marketing

The customer/user agrees to the use by the Bank of customer or user data from E-Banking for internal marketing purposes. Regarding the handling of customer data, reference is made to the "General Conditions" and the "Privacy Statement" of the Bank. This can be viewed on the Bank's website at [www.cler.ch/datenschutzerklaerung](http://www.cler.ch/datenschutzerklaerung).

## 11. Termination

Agreements for E-Banking can be terminated in writing at any time by the customer and the Bank. The Bank is entitled at its own discretion to cancel existing agreements for E-Banking and thus access to the E-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 it has no longer been used for more than one year.

## 12. Reservation of particular statutory provisions

Any statutory or other provisions regulating the operation and use of the internet remain reserved and apply to existing agreements for E-Banking from their commencement.

## 13. General Conditions

13.1 The Bank's General Conditions also apply to the use of bank services in E-Banking.

## 14. Partial invalidity

The invalidity, illegality or unenforceability of individual or more provisions contained in these terms and conditions shall not affect the validity of the remaining contractual provisions.

## 15. Amendment of the terms and conditions for E-Banking

The Bank may amend the terms and conditions for and the offer of E-Banking at any time. It shall notify the customer/user in a suitable way. Amendments shall be deemed to be approved if the customer/user does not comment on the amendments to the terms and conditions and/or services within a period of one month following notification.

## 16. Mobile Banking

The above terms and conditions for E-Banking also apply to Mobile Banking services. Any variations arise from the terms and conditions in the "Information on E-Banking".

Version: January 2020