K&H Bank Zrt.

1095 Budapest, Lechner Ödön fasor 9.
phone: (36 1) 328 9000,
fax: (36 1) 328 9696
www.kh.hu • bank@kh.hu

GENERAL CONTRACTING TERMS AND CONDITIONS
FOR BANKING SERVICES REQUIRING ELECTRONIC IDENTIFICATION

These GCTC have been amended due to the modification of rules concerning access to Banking Services Requiring Electronic Identification. The modifications are highlighted in yellow.

Effective as of February 9, 2018
(date of entry into force postponed from November 26, 2017)

K&H Bank Zrt. (registered office: 1095 Budapest, Lechner Ödön fasor 9., company registration number: Cg. 01-10-041043, registered by: Metropolitan Court as Court of Registration, hereinafter: "Bank") shall provide Banking Services Requiring Electronic Identification to its Clients in accordance with these General Contracting Terms and Conditions (hereinafter: "GCTC").
The personal scope of these GCTC shall extend to all persons using Banking Services Requiring Electronic Identification as defined in Section 1 below.

The provisions of these GCTC shall apply:

- to all Users using K&H e-banking services with an electronic identification device who signed their contracts before or on 18 September 2009;
- to all Users using K&H e-banking services with SMS authentication who signed their contracts before or on 18 September 2009 and who are already using such services with the new electronic identification process as per the notice sent by the Bank (K&H myID, ePIN code, primary SMS password);
- to all Clients who have used the services of the K&H TeleCenter (Retail Telephone Banking)/ Cégvonal (SME Telephone Banking)/Corporate Customer Service (Telephone Banking) actively as per the definition of the Bank (i.e. at least once since 1 January 2008) and who are now using them by way of the new electronic identification process as per the notice sent by the Bank (K&H myID, ePIN code);
- to all Clients not using the K&H Retail/SME/Corporate Telephone Banking Services actively who have switched to Banking Services Requiring Electronic Identification as per the notice sent by the Bank and who are thus using these services by way of the new electronic identification process (K&H myID, ePIN code); and
- to all Clients having signed their contracts for Banking Services Requiring Electronic Identification after 18 September 2009.

1. DEFINITIONS

1.1. Client:
Natural persons over 18 years of age or, in the case of certain products, over 14 years of age; resident and non-resident legal or unincorporated entities; organisations (foundations, churches, associations, municipalities, etc.); businesses; or private individuals engaging in commercial activities that have a contract in place with the Bank for services provided by credit institutions to which the Banking Services Requiring Electronic Identification applies.

1.2. Agent:
A natural person identified by the Client in the Contract prior to November 2, 2016 who can avail themselves of the services offered by the K&H Corporate Telephone Banking Service in the manner specified in the prevailing Announcement following a successful telephone authentication. Only a Client who is a resident or non-resident legal or unincorporated entity, organisation (foundation, church, association, municipality, etc.), business or private individual engaging in commercial activities may have an Agent.

1.3. Telephone Representative:
A natural person identified by the Client in the Contract prior to November 2, 2016 who liaises between the Bank and the Client in respect of the services available through the K&H Corporate Telephone Banking Service, acts on the Client's behalf and may use the services defined in the prevailing Announcement following a successful telephone authentication. Only a Client that is a resident or non-resident legal or unincorporated entity, organisation (foundation, church, association, municipality, etc.), business or private individual engaging in commercial activities may have a Telephone Representative. The person of the Telephone Representative is not necessarily the same as the person with power of agency as defined in the relevant laws, i.e. the legal representative.

1.4. Disponer:
A User identified prior to November 2, 2016 by a Client that is a resident or non-resident legal or unincorporated entity, organisation (foundation, church, association, municipality, etc.), business or private individual engaging in commercial activities, who is a signatory towards the Bank and is entitled to use the services requiring a right of disposal as specified by the Client and defined in the prevailing Announcement, following a successful telephone authentication, through the K&H Corporate Telephone Banking Service.

1.5. Transacting Person:
A natural person identified by the Client in the Contract prior to November 2, 2016 who may use the services available through the K&H SME Telephone Banking Service specified by the Client and defined in the effective Announcement following a successful telephone authentication.

1.6. Right of disposal:
A collection of powers and rights that define the accounts with respect to which, the channels through which and the methods in which a User is entitled to transact, as well as the types of transactions a User is entitled to execute. A right of disposal may extend to one of the following: (i) execution of financial and non-financial transactions, or (ii) execution of non-financial transactions only. The available transactions are defined for each channel and each account type in the relevant Announcement.

1.7. e-bank User:
In the case of K&H corporate e-banking services, a natural person authorised - by a Client that is a resident or non-resident, legal or unincorporated entity, organisation, (foundation, church, association, municipality, etc.), business or private individual client engaging in commercial activities - to carry out electronic banking transactions defined in the Contract in accordance with the terms and conditions applicable to the service. E- bank users with different powers can be defined in the Contract. The exact content of the different powers is described in the Users' Manual.

1.8. Electra User:
A natural person authorised by a non-natural-person Client using the Electra service and K&H Electra24 electronic banking service based on a mobile phone application, to execute banking transactions requiring electronic identification in accordance with the terms and conditions applicable to the service concerned, appointed by the Client in the relevant Annex.

1.9. mobile bank User:
In the case of the K&H mobile banking service, a natural person authorised to execute electronic banking transactions - according to the terms and conditions applicable to the service – by a resident or non-resident legal or unincorporated entity, organisation (foundation, church, association, municipality, etc.), business or private individual client engaging in commercial activities.

1.10. e-post User[1]:
A User authorised – under the terms and conditions defined in the relevant Announcement – by a non-natural-person Client to execute banking transactions requiring electronic authorisation through the K&H e-post service, in accordance with the terms and conditions applicable to this service, designated by the Client in the relevant Annex. We differentiate between Normal Reader and Confidential Reader users. The powers relating to these roles are defined in the Announcement for Corporate Clients. After November 2, 2016, user authorisations that can be defined in the K&H e-post service are contained in the Announcement for Corporate Clients.

1.11. Mobile Wallet User:
A mobile bank User who has accepted the terms of use of the mobile wallet.

1.12. User:
A natural person authorised by the Client under the terms relevant to the service and under the conditions specified in the relevant Announcement for using Banking Services Requiring Electronic Identification and executing electronic banking transactions.
Instead of the Agent, Telephone Representative, Disponer, Transacting Person Client roles, the rights of disposal defined in Chapter III. Services and Annex 11 of the Announcement for Corporate Clients can be given to Users specified after November 2, 2016.

1.13. Banking Services Requiring Electronic Identification:
A collective name for the services provided by the Bank and defined below:

- **K&H e-banking services:** banking services provided by the Bank and available to Clients online, i.e. the services available to Clients on the website of the Bank, https://wwww.kh.hu/ebank. Natural person Clients must use the services themselves as they are not entitled to appoint a Permanent Proxy. The available services are listed in the latest effective Announcements.
- **K&H mobile bank:** A banking service provided by the Bank and available on a mobile device to clients using the K&H e-

[1] also referred to as "e-box User"

bank service, or to e-bank Users. The K&H mobile bank service is available to all K&H e-bank Users. A list of the services available to clients and the technical requirements for the use of such services are contained in the prevailing Announcements.

- **K&H mobile wallet:** The K&H mobile wallet is an integral but distinct part of the K&H mobile bank application. It contains our digital bankcard payment services and the related functionalities. The K&H mobile wallet can be accessed via mobile devices which meet the technical parameters published in the Announcement.
- **Electra service:** a banking service provided by the Bank to non-natural-person Clients through an electronic system installed on the Client's computer or accessible via the Internet, suitable for the execution of banking transactions requiring electronic identification specified in Section 18.7.1.
- **K&H Electra24 electronic banking service based on a mobile phone application**: A banking application provided by the Bank and available for use on mobile devices by customers using the Electra service, through which banking transactions requiring electronic identification, as set out in the present GCTC and in the current Announcement, can be initiated.
- **K&H e-post service[2]:** electronic bank mailbox service provided by the Bank through the Internet to the Users of non-natural-person Clients, through which Users may use the services specified in the Announcement.
- **K&H TeleCenter:** telephone banking services provided by the Bank to natural person Clients through a telephone customer service. A Permanent Proxy or a Co-holder may act in the Client's place or on their behalf if necessary, using their personal K&H myID and ePIN code.
- **K&H SME/Corporate Telephone Banking Service:** telephone banking services provided by the Bank to non-natural-person Clients through a telephone customer service. The two customer services differ in terms of the services they provide. The services available from these two customer services are described in the prevailing Announcements.

1.14. K&H myID:
The eight-digit numeric identification code defined in the manner described in Section 3 for the unique identification of the User when using the Banking Services Requiring Electronic Identification.

1.15. ePIN code:
The secret six-digit numeric identification code defined in the manner described in Section 4 which, together with the K&H myID, serves to uniquely identify the User when using the Banking Services Requiring Electronic Identification.

1.16. User name:
An alphanumeric identification code defined in the manner described in Section 5 for the unique identification of the User when using the K&H e-bank and the K&H e-post services.

1.17. Password:
An alphanumeric identification code defined in the manner described in Section 6 for the unique identification of the User when using the K&H e-bank and the K&H e-post services.

1.18. Electronic identification:

- Identification with K&H myID: Electronic identification without a device for the use of Banking Services Requiring Electronic Identification. The K&H myID is to be used together with the ePIN code or, in the case of K&H e-banking requiring SMS authentication or in the case of the K&H e-post service, the primary SMS password upon the first use. When activating the K&H mobile bank services with the use of the myID, both the K&H myID and the ePIN code should be provided.
- Identification with a User name: For accessing the K&H e-bank by an e-bank User or the K&H e-post services by an e-post User through SMS authentication, their user name, password and primary SMS password should all be provided. When activating the K&H mobile bank services with the use of the User name, both the User name and the password should be provided.
- Identification with a chip card as identification device: e-bank Users may opt to identify themselves with the help of an identification device when using K&H e-banking services or jointly using K&H e-bank and K&H e-post services, in which case the Bank shall provide an identification device and a chip card reader to them. Chip card identification device and chip card reader is not available for bank accounts opened from 16th October 2017.
- Identification with Token as identification device: For the use of the Electra service or the joint use of the Electra service and the K&H e-post service, the Bank provides Electra Users with an identification device, a Token. In order to use the service(s), Users must authenticate themselves with their Token together with the matching Token password.

[2] also referred to as "K&H e-box service"

- Identification with smart phone application (VICA): For using the webElectra service and K&H Electra24 electronic banking service based on a mobile phone application, the Bank (also) allows the identification of the relevant Electra User via a smart phone application. Using the PIN provided for the application, the Electra User can log on to the application and execute banking transactions requiring electronic identification, accessible for the application in question.
- Identification with a mobile token device: It means the use of an electronic identification device available to the e-bank and/or the mobile bank Users in the K&H mobile bank application to access the Bank's e-bank and mobile bank services and to sign transactions launched in such interfaces. The application is protected by an mPIN consisting of 5-12 characters, defined by the User when activating the mobile token. Fingerprints can also be used for authentication if allowed by the mobile device used.

1.19. Contract:
A unique Contract concluded by and between the Client and the Bank for the use of Banking Services Requiring Electronic Identification. The annexes (hereinafter: the Annex), these GCTC, the Bank's General Terms and Conditions of Business and the relevant Announcements form an integral part of the Contract.

1.20. Framework Agreement:
A Contract between the Parties on Banking Services Requiring Electronic Identification subject to these GCTC can be concluded in the form a framework agreement on the provision of banking services, under the terms and conditions defined therein. In this case, the "Framework Agreement" and the related "Service request and/or modification" documents shall together mean the Contract on the provision of Banking Services Requiring Electronic Identification. A list of services available under the Framework Agreement is contained in the latest effective Announcement.

1.21. Announcement:
Notices displayed in the public areas and on the website of the Bank setting out the terms and conditions of using the Banking Services Requiring Electronic Identification pursuant to these GCTC: (i) Announcement on the bank accounts, deposit accounts, term deposits and cash transactions of private individual customers, and (ii) Announcement on the bank accounts, deposits, cash transactions, bankcards and investments of private banking customers, and (iii) Announcement on the bank accounts, deposits, cash transactions, bankcards and investments of premium banking clients, and (iv) the announcement on the K&H retail credit card, as well as (v) Announcement for Corporate Clients. Among others, Announcements describe the contents of the relevant services, the specification of the devices required for their use and the applicable fees and charges.

1.22. Mobile token:
A login device embedded in the K&H mobile bank application, which gives access to K&H e-bank, e-post, and mobile bank services after it has been downloaded and activated.

1.23. mPIN code:
A secret numeric identification code provided by the User upon activation and required for identification when accessing the K&H mobile bank, K&H e-bank and K&H e-post services through the use of a mobile token.

1.24. Fingerprints (for iPhone: TouchID): If using the mobile token when accessing the K&H mobile bank, K&H e-bank and K&H e-post services, Users can choose upon activation to use their fingerprints, if allowed by their mobile device (biometric authentication), instead of the mPIN code for authentication. Fingerprint authentication requires the use of fingerprints saved in the mobile device. The use of fingerprints is supported by the application only for certain device types that are listed in the prevailing Announcement.

1.25. Wallet PIN:
Numeric identifier used to authorize mobile payments on mobile devices. It is provided by the K&H mobile wallet User when the first bankcard is digitized and it can be changed freely at a later date. The same wallet PIN is associated with all the digital bankcards connected to a mobile device and different wallet PINs may be used on different devices.
Merely entering the wallet PIN does not qualify as full-scale electronic identification. It is used to authorize transactions only.

1.26. Unique definitions pertaining to the K&H e-banking services:

Identification device (chip card): a plastic card issued by the Bank not to be construed as a bank card. Acting as an electronic means of payment providing remote access, the card and its matching PIN code allow the given User to use both the K&H e-bank service and the K&H e-post service through the Internet. The identification device issued by the Bank is the property of the Bank. Only natural persons may hold identification devices. One natural person may only have one identification device at a time.

Chip card PIN code: a secret numeric identification code generated by the Bank for the identification device, required for chip card identification when using the K&H e-banking/K&H e-

post services. The PIN code of this identification device is different from the ePIN code.

Primary SMS password: One-time password sent by the Bank to the Client in an SMS message upon login, authorising the User for one login.

Secondary SMS password: For each transaction initiated by the Client, the Bank sends an SMS message to the Client containing a unique one-time password at the time when (a) transaction(s) is/are to be performed.

User's Manual: a manual supporting the use of the e-banking service, giving a detailed description of the process of executing the different transactions, the content of the different functions and powers and the features of the different specifications.

Access right: A right bestowed upon the e-bank User by the Client, granting the e-bank User the right to execute electronic banking transactions on the Client's account specified in the relevant Annex to the Contract, in line with the terms and conditions applicable to the service and in compliance with the provisions laid down in the Contract. The Client grants access rights to e-bank Users and determines the extent thereof in the relevant Annex to the Contract.

Driver: The program required for the operation of the chip card reader.

Minimum configuration: The minimum technical conditions required for the use of the service.

Operation in public places: Operation in any places other than the places where the computer of the Bank or of the User are operated.

Chip card reader: A physical device needed for the use of the K&H e-banking services requiring chip card identification.

1.27. Unique definitions pertaining to the K&H mobile bank service:

mobile device: a smart phone with an operation system of the version and type as defined in the prevailing Announcement, and Internet access.

mobile banking system: the Bank's electronic system suitable for the execution of Banking Transactions Requiring Electronic Identification, accessible in the context of the mobile banking service.

mobile banking software: a mobile device application enabling the User to execute Electronic Banking Transactions, i.e. to use the Bank's services.

Electronic Banking Transaction: any and all queries, orders and notifications given by the User to the Bank electronically. In electronic banking transactions, the User's signature is substituted with an identification code given in the format approved by the Bank.

1.28. Unique definitions pertaining to the K&H mobile wallet

NFC (Near Field Communication): Data transmission solution which enables mobile devices in each other's proximity to communicate with each other. The K&H mobile wallet can only be used on mobile devices capable of such communication for the User's device and the POS terminal must be able to exchange information.

In addition to this present section, the definitions set forth in the bankcard services GCTC (General Contracting Terms and Conditions of Bank Card and Credit Card Services) are also applicable to the K&H mobile wallet service.

1.29. Unique definitions pertaining to the Electra service and K&H Electra24 electronic banking service based on a mobile phone application:

Identification device (Token): a physical device issued by the Bank, which together with its matching Token password allows only the given Token holder User to use the Electra service. The Token issued by the bank is the property of the Bank. Only natural persons may be holders of a Token. One natural person may only have one Token at a time.

Token password: an 8-character identification code specified by the User at the time of the first login using the Token, which has a dual function. It shall be used on the one hand at the time of each login during the use of the Electra service and on the other hand, for the approval of Electronic Banking Transactions performed in the context of the Electra service (by Electra Users to whom the right of disposal was granted using the form provided in the relevant Annex).

webElectra: the web-based interface of the Electra service.

VICA: an application developed for Android and iOS operating systems which enables the user to confirm or decline access or signatory actions initiated on the web platform or via a mobile device while using the service.

Electra System: the Bank's electronic system for the execution of Banking Transactions Requiring Electronic Identification available in the context of the Bank's Electra service and K&H Electra24 electronic banking service based on a mobile phone application.

Electra Software: any and all of the computer programs enabling the Electra User to execute Electronic Banking Transactions – and thereby to use the Bank's services, irrespectively of the application/device used.

Electra Software Module: all of the services requested by the Client and set up by the Bank from among the ones listed in Section 18.7.1.

Electronic Banking Transaction: all orders and notices provided to the Bank by the Electra User directly through the application of computer communication, at least partly in the form of electronic signals. During Electronic Banking Transactions, the Electra User substitutes their signature with personal identification coding in the format approved by the Bank or with another similar authorisation tool (approved by the Bank). Orders and notices provided as Electronic Banking Transactions are irrevocable and non-modifiable unless these GCTC expressly stipulates otherwise or agreed otherwise by the Parties.

ERP software: (ERP = enterprise resource planning) means the Client's own accounting and account management applications. Most ERP software applications are able to issue invoices (payment orders) and import them into Internet banking systems as well as electronically receive bank account statements for the purpose of automatic verification.

mobile device: an Internet-enabled smartphone with the version number and operating system stipulated in the relevant Announcement.

1.30. Unique definitions pertaining to the K&H e-post service:

Identification device (Token): A physical storage device issued by the Bank, which together with its matching Token password allows only the given Token holder User to use the K&H e-post service. The Token issued by the bank is the property of the Bank. Only natural persons may be holders of a Token. One natural person may only have one Token at a time.

Token password: An 8-character identification code specified by the User at the time of the first login using the Token, which shall be used at the time of each login during the use of the K&H e-post service.

Identification device (Chip card): a plastic card issued by the Bank, not to be construed as a bank card. Acting as an electronic means of payment providing remote access, the card and its matching PIN code allow only the given User to use both the K&H e-bank service and the K&H e-post service through the Internet. The identification device issued by the Bank is the property of the Bank. Only natural persons may hold identification devices. One natural person may only have one identification device (chip card) at a time.

Chip card PIN code: a secret numeric identification code generated by the Bank, required for chip card identification when using the K&H e-banking/K&H e-post services. The PIN code of the chip card is different from the ePIN code.

Primary SMS password: One-time password sent by the Bank to the User in an SMS message upon login.

Electronic Banking Transaction: All queries, orders and notices provided to the Bank by the User directly through the application of computer communication, at least partly in the form of electronic signals. During Electronic Banking Transactions, the User shall substitute their signature with a personal identification coding in the format approved by the Bank.

Access right: The right granted by the Client to the e-post User on the basis of which the e-post User disposes over the account or accounts specified by the Client and is authorised to perform Electronic Banking Transactions. The Client specifies the access rights of e-post Users for the Bank using the form provided in the relevant Annex.

2. GENERAL PROVISIONS

2.1. Clients can request Banking Services Requiring Electronic Identification in a Contract signed with the Bank for this purpose, under which Users may use the banking services specified in the Announcement pertaining to the selected electronic channel, using their K&H myID. The Bank issues a K&H myID, an ePIN code and a K&H e-bank identification device and a matching PIN code or an SMS password to be used for the services.

2.2. Issues not regulated in these GCTC shall be governed by the provisions of the Bank's General Terms and Conditions of Business and the General Contracting Terms and Conditions applicable to the services used by the User. Furthermore, issues not addressed herein shall be subject to the provisions of the Civil Code and the prevailing legislation on credit institutions, investment enterprises, payments and electronic payment channels. In addition, the User expressly confirms and accepts the provisions set out in Section 4: Data protection, data handling and the provision of information of the Bank's General Terms and Conditions of Business, and grants the Bank the powers described therein.

2.3. The use of the services is subject to the fees, commissions and charges set out in the relevant Announcements. The Bank shall be entitled to charge to the Client's account the fees, commissions and charges at the time

specified in the relevant Announcements. The fees, commissions and charges payable for the Banking Services Requiring Electronic Identification quoted in the relevant Announcements do not include the fees, commissions and charges payable for the transactions effected while using the services. The costs associated with the use of the devices required for the use of the Banking Services Requiring Electronic Identification (telephone, Internet, etc.) shall not be payable by the Bank.

When applying for Banking Services Requiring Electronic Identification or in the case of already used Banking Services Requiring Electronic Identification, in the absence of a bank account used for the settlement of fees (fee settlement account) the Bank shall automatically designate, as fee settlement account, the Client's live, non-dedicated bank account that was opened at the earliest, according to the order defined in the relevant Announcement. Any time during the provision of Banking Services Requiring Electronic Identification, the Client may request a modification of their fee settlement account in a branch. The method of designating the fee settlement account, and the accounts eligible for being involved in the fee settlement are contained in the latest effective relevant Announcement. In the absence of a fee settlement account, the Bank is entitled to terminate the Contract on Banking Services Requiring Electronic Identification.

2.4. When a User is initiating an order or executing a banking transaction, the time when the service was requested shall be the time determined and recorded by the electronic system of the Bank. The Bank shall execute the orders placed via the Banking Services Requiring Electronic Identification within the timeframe specified in the relevant Announcements concerning the procedures of receiving and executing Orders.

2.5. The Client shall honour their payment obligations to the Bank arising under these GCTC as they become due/as they occur. The Bank shall have the right to charge any amounts receivable from the Client to any of their accounts managed by the Bank, or to offset such amounts against any amounts due to the Client on another account or from the Bank.

2.6. The Client undertakes to pass on the contents of the GCTC to the User identified by them during the use of the service.

2.7. Each User shall have their unique K&H myID, which can only be used by them. Users shall be bound by the obligations of the Client set out in the GCTC.

2.8. The User shall acknowledge the instructions given while using the service as per the GCTC following the identification procedure as their own, and they shall take full responsibility for such instructions.

2.9. The Bank does not provide investment advice regarding orders given via Banking Services Requiring Electronic Identification, thus the Bank does not examine the suitability and appropriateness of the product in question for the Client.

2.10. Banking Services Requiring Electronic Identification are provided in the Hungarian language, but the e-bank and mobile bank services are also available in the English language. The User can only give orders in other languages at their own responsibility.

3. COMPOSITION OF THE K&H myID AND HOW TO OBTAIN IT

3.1. All new Users shall receive their own K&H myID from the Bank. Natural persons may obtain their new K&H myID in a branch or via the K&H TeleCenter (Retail Telephone Banking Service), while legal and unincorporated entities may obtain their new K&H myID in a branch only.

4. COMPOSITION OF THE ePIN CODE AND HOW TO OBTAIN IT

4.1. All new Users shall receive their own ePIN code. The ePIN code can be set up in a branch as a series of numbers determined by the User or generated in advance by the Bank in a closed system. The latter ePIN code type can also be mailed to the User upon request (for details see the effective Announcement).

5. COMPOSITION OF THE USER NAME AND HOW TO OBTAIN IT

5.1. Each User using the K&H e-bank or K&H e-post service by SMS authentication after July 15, 2013 shall provide, upon their first login, an alphanumeric user name composed of minimum 6 and maximum 15 characters, with which they can later use the service. A User shall use the same user name for accessing the K&H e-bank and the K&H e-post services.

Format requirements:

- minimum 6, maximum 15 characters
- no differentiation between small and capital letters is made
- may contain numeric and alphabetic characters
- only the characters of the English alphabet are allowed
- of special characters, the underline and the dot are allowed
- spaces are not allowed.

6. COMPOSITION OF THE PASSWORD AND HOW TO OBTAIN IT

6.1. Each User using the K&H e-bank or the K&H e-post service by SMS authentication after July 15, 2013 shall provide, upon their first login, an alphanumeric password belonging to their user name described in Section 5, composed of minimum 8 and maximum 15 characters, with which they can later use the service. A User shall use the same password for accessing the K&H e-bank and the K&H e-post services. Users are obliged to modify their password at the intervals defined in the relevant Announcement.

Format requirements:

- minimum 8, maximum 15 characters
- small and capital letters are differentiated
- 3 consecutive identical characters are not allowed
- the password cannot be the same as the user name
- it must contain small and capital letters alike, and at least two numbers

7. COMPOSITION OF THE MPIN CODE AND HOW TO OBTAIN IT

Each User using the K&H e-bank services through mobile token authentication or the K&H mobile bank shall provide, upon activation (after they have downloaded the relevant application), a numeric mPIN code composed of minimum 5 and maximum 12 characters, which allows them to use the services later on (instead of the mPIN code, fingerprints can also be used for authentication if made possible by their mobile device). For activation, either the user name and password defined in Sections 5 and 6 or the K&H myID and ePIN code defined in Sections 3 and 4 must be used. Or, if such identification data are not available, Users can activate their mobile token in the K&H e-bank.

8. COMPOSITION OF THE WALLET PIN AND HOW TO OBTAIN IT

Having accepted the terms of use of the K&H mobile wallet service, for the digitization of the first bankcard Users will be required to choose a numeric wallet PIN of min four (4) but max eight (8) digits, which will serve to authorize mobile payments. Later, the wallet PIN can be freely changed.

9. USE OF FINGERPRINTS

If their mobile device allows, the User may choose to use their fingerprint(s) saved on their mobile device for mobile token authentication as means of biometric authentication.

10. ACCESS TO AND MODIFICATION OF BANKING SERVICES REQUIRING ELECTRONIC AUTHENTICATION

10.1. The Client shall specify the Banking Service(s) Requiring Electronic Identification they wish to use in the relevant Annex to the Contract, upon which the Bank shall grant access to the User thereto. An exception to this is the K&H mobile bank service, which is automatically made available to Clients also using the K&H e-bank service; and the K&H mobile wallet service, which is automatically made available to K&H mobile bank Users, provided they meet the technical parameters.

10.2. The Bank shall provide the K&H myID to the User after the signature of the Contract. The Bank shall be entitled to withhold the K&H myID, the ePIN code and the identification device until the Client has complied with all the terms and conditions pertaining to the requesting of the services in question or to putting the authorisation into effect and with any other terms and conditions set out in the Contract.

10.3. The User shall be entitled to change their personal ePIN code in the automated telephone system. The PIN code of the identification device can be changed in the e-banking application. mPIN codes that belong to the mobile token may be modified by the User in the K&H mobile bank application. This is also where the User can specify whether they want to use their fingerprint (if allowed by their mobile device) or the mPIN code for mobile token authentication.

Users having signed in and been identified in the mobile bank can change the wallet PIN in the K&H mobile wallet.

10.4. The User shall be responsible for their K&H myID and ePIN code and their identification device and the matching PIN code from their receipt or creation in the system.

11. PROCEDURES TO BE FOLLOWED BY THE USER; ELECTRONIC IDENTIFICATION, AND VERIFICATION OF ENTITLEMENT

11.1. If the User fails to comply with all the rules and requirements applicable to electronic identification as set out herein, the Bank shall be entitled to refuse to provide the requested service.

11.2. Prior to their electronic identification, Users can only carry out transactions which are not subject thereto according to the relevant Announcement.

11.3. Users must enter their K&H myID and ePIN code when using Banking Services Requiring Electronic Identification; their primary/secondary SMS password when using K&H e-banking or K&H e-post services requiring SMS authentication; their

identification device and matching PIN code when using K&H e-banking services or jointly using K&H e-banking and K&H e-post services requiring identification by an identification device; their mPIN code (or fingerprint(s) if their mobile device allows the use of fingerprints) when using K&H e-bank and K&H e-post, or K&H mobile bank requiring authentication through a mobile token, or their identification device and matching Token password when using the Electra service or K&H e-post service requiring Token-based authentication. When using webElectra or K&H Electra24 electronic banking service based on a mobile phone application, electronic identification takes place by using the VICA smart phone application linked to the K&H myID of the Electra User concerned and by providing the PIN of that application. For the K&H mobile wallet service, a User's entitlement to authorize mobile payments is verified by the use of the wallet PIN

11.4. The handling of ePINs, mPINs, wallet PINs, and PIN codes by the Bank is subject to strict security requirements.

11.5. Identification on landline or mobile telephone (K&H TeleCenter (Retail Telephone Banking Service), K&H SME Telephone Banking Service, and K&H Corporate Telephone Banking Service):

Having successfully reached the relevant telephone banking service, the User must enter their K&H myID code and their ePIN code on a touch-tone or mobile telephone. Once they have been successfully identified, they are put through to the automated system or a Telephone Banker or a staff of the K&H Corporate Telephone Banking Service who will assist them with the execution of their order.

11.6. Online authentication for K&H e-banking services:

- Accessing the K&H e-banking services with SMS authentication: the User keys in their K&H myID and ePIN code using the keyboard. The Bank sends the primary SMS password to their mobile phone in a text message. Only when all three codes have been entered can the User use the K&H e-banking services. If a User logs in for the first time after July 15, 2013, they shall provide the user name and password described in Sections 5-6, which shall replace the K&H myID and the ePIN code in all subsequent login actions.
- Accessing K&H e-banking services with an identification device: the User inserts the identification device in the chip card reader according to instructions and then keys in their PIN code. The services will be accessible after a successful authentication of the correctly entered code.
- Accessing the K&H e-bank with mobile token authentication: After selecting the Login function on the K&H mobile bank home page the User uses the camera of their mobile device to scan the coloured code displayed on the computer screen. After successfully scanning the code, they enter the mPIN code on their mobile device. If accepted, the identification is deemed completed and the service becomes available. In case the User's mobile device has no Internet connection when logging in the User must first scan the coloured code and enter the mPIN code and then key in the 19-character login code (a numeric code consisting of 19 characters) in the appropriate field of the e-bank screen, so the joint provision of both the mPIN code and the login code allows the User to access the K&H e-bank service.

11.7. Authentication for the K&H mobile banking service

- Login to the K&H mobile banking service: the Users can access the K&H mobile banking service after providing their mPIN code entered upon activating the application or their fingerprint(s) if their mobile device allows the use of fingerprints.

11.8. Authentication for the K&H mobile wallet service

- To enter the K&H mobile wallet service Users need not be identified. However, certain functionalities will only be accessible after the User has logged in to the K&H mobile bank. The wallet PIN is used to authorize mobile payments only.

11.9. Authentication for Electra and K&H Electra24 electronic banking service based on a mobile phone application:

After the insertion according to the instructions of the Token in the USB connector, the Electra User keys in the Token password using the keyboard. After the correct entry of the Token password, the authentication is successful and the Electra service becomes accessible. When using the K&H webElectra service, the service also becomes accessible with the help of the VICA application installed on the smart phone by the Electra User. K&H Electra24 electronic banking service based on a mobile phone application, can only be used with the VICA application installed by the Electra User onto his/her smartphone. For using the downloaded VICA application, the Electra User keys in the registration code provided by the Bank and the one-time SMS code sent by the Bank; once these codes are entered the application is activated. In the activated application, the Electra User must choose a PIN code which will have to be used in the future to start the VICA application and to validate the transactions. From then on, the Electra User logs in the VICA application by indicating their PIN registered earlier and confirms the identification requests appearing there.

11.10. Authentication for K&H e-post services:

- The e-bank User using K&H e-banking services may access the K&H e-post service after accessing the e-bank.
- Accessing the K&H e-post service with SMS authentication: the e-post User keys in their K&H myID and ePIN code using the keyboard. The Bank sends them the primary SMS password to their mobile phone in a text message. Only when all three codes have been entered can the User use the K&H e-post service.
- Accessing the K&H e-post service with an identification device (chip card): the e-bank User inserts the identification device in the chip card reader according to instructions and then keys in their PIN code. The K&H e-bank and the K&H e-post services will be accessible after a successful authentication of the correctly entered code.
- Accessing the K&H e-post service with an identification device (Token): After the insertion according to the instruction of the Token in the USB connector, the e-post User keys in the Token password using the keyboard. The authentication is successful and the e-post service is accessible after the correct entry of the Token password.

11.11. When web-based Banking Services Requiring Electronic Identification (K&H webElectra, K&H e-bank, K&H e-post) are used, once identification is successfully completed using one of the electronic identification methods stipulated for the relevant channel and described under Sections 11.6, 11.9 and 11.10, on the same device the User will be able to access, without further identification, all other web-based electronic channels to which it has user access either as a Client, or having been authorised by a Client (log-on with one-off identification). However, the approval of a transaction requiring electronic identification may, in each and every channel, only take place if electronic identification is successfully completed using the identification device stipulated for the relevant channel, and, if the identity of the Client and the User is different, approved by the Client for use by the User.

12. GENERAL RIGHTS AND OBLIGATIONS OF THE PARTIES

12.1. The User shall always act during the term of the Contract signed with the Bank as can be reasonably expected in such circumstances. This includes an obligation to retain their K&H myID and ePIN code and the identification device and PIN code required for authentication. Further, the Users shall keep confidential the items listed above as well as their user name and password, their primary/secondary SMS password, their login code and numeric codes used for signing transaction orders if relying on mobile token identification, and the mPIN code and may not disclose them to third parties. Mobile wallet Users are required to also handle confidentially and not to disclose to third parties the wallet PIN they use to authorize transactions and may not disclose them to third parties. Should a User make a note of their K&H myID and ePIN code, or their primary/secondary SMS password and the PIN code for their identification device, or the user name and the password, or the mPIN or wallet PIN, they shall keep such records separate from any and all documents associated in any way with their bank accounts or their identification device or their smart phone having the K&H mobile bank application downloaded, and they shall seek to ensure that they cannot be accessed and acquired by third persons. The User shall be responsible for the safe handling and the proper and lawful use of their identification device, chip card reader, K&H myID, PIN codes, user name and password. The User shall be fully liable for any damages resulting from their failure to comply with the above fully or in part. Furthermore, the User shall be liable for any direct and consequential damages resulting from the incorrect use of their K&H myID, ePIN code, primary/secondary SMS password, user name and password, the mPIN code/fingerprint, the wallet PIN, the identification device, PIN code and chip card reader or the obtaining thereof by third persons. The Bank shall accept no liability for any damage resulting from the circumstances described herein.

12.2. The Bank shall use all reasonable efforts in its electronic data transmission to ensure that the Client's details cannot be accessed by unauthorised persons. The Client acknowledges that the Bank shall not be liable for any damages arising from data becoming accessible by a third person despite the Bank's reasonable efforts to prevent this.

12.3. In the case of K&H e-banking and K&H e-post services requiring SMS authentication, as well as regarding the confirming SMS message when activating the K&H mobile banking service with the combination of myID/ePIN or user name/password, the liability of the Bank shall extend from sending the message from the Bank through to its arrival to the message centre of the relevant mobile network operator.

12.4. Irrespective of the User's liability stipulated in Section 12.1 the Bank, in accordance with its statutory obligation, must refuse to provide the relevant service if it discovers that the User's K&H myID, ePIN code, primary/secondary SMS password, identification device and chip card PIN code, activated mobile token and related mPIN code, user name and related password, or wallet PIN have been lost by or stolen from the User. The Bank must prohibit the provision of services requested in this manner at the time and thereafter, delete the ePIN code

and cancel the identification device, the user name and the related password, and the mobile token and the related mPIN code, as well as the wallet PIN, and promptly notify the Client thereof in the most practicable manner, in most cases by telephone or, if that fails, by e-mail, fax or post. In the event that a mobile token identification code is cancelled due to alleged misuse/abuse, the Bank will also suspend the related mobile wallet service.

12.5. The Bank shall be entitled to refuse to execute a User's order if it does not comply with the legislative provisions in effect, is incomplete, incorrect or contains other incorrect data, and at the same time it shall inform the User of the reason(s) thereof. The Bank shall not be responsible for events and non-performances arising from the fact that the User fails to use their K&H myID, identification device and chip card reader, or the mobile token and the mPIN code/fingerprint, or the wallet PIN, or use them incorrectly or not in the environment required for their correct use. Environment for correct use shall mean the tools specified in these GCTC or the relevant Announcement, the components of the installation program provided by the Bank and the technical environment suitable for their regular use at the time.

12.6. The Bank shall accept and handle the orders received via the system for Banking Services Requiring Electronic Identification and record them in its computerised system, if they meet the same requirements in terms of their content as orders given in writing. The recorded entry substitutes the written order and it is the equal thereof in every respect. Orders received electronically may however be different from the written order in terms of data content, final submission deadline, execution order and fees and commissions, the details of which are described in the relevant Announcement. The Client shall accept the data recorded in the system of the Bank as authentic and recognise them as evidence of both giving and executing the order in the event of a legal dispute.

12.7. In the case of services used according to the GCTC, the User shall recognise the information provided after the authentication as their own and they shall take full liability therefor.

12.8. The Bank shall be entitled to refuse to execute orders if a technical error occurred during their entry and the User did not confirm the order and/or its execution as a result.

12.9. The Bank shall not be liable for any technical errors occurring during the provision of the services or the failure of transactions resulting therefrom if such errors occurred outside the control of the Bank or cannot be attributed thereto.

12.10. To take advantage of Banking Services Requiring Electronic Identification Users must be able to provide:

- their K&H myID and ePIN code,
- their user name, the related password, and the primary/secondary SMS password,
- their identification device and the PIN code,
- the activated mobile token and the mPIN code/fingerprint, and
- the wallet PIN.

The Bank shall not check the User's authority for and the circumstances of their use of the K&H myID and the ePIN code, or the user name and the password and the SMS password, or the identification device and the PIN code, or the mobile token and the mPIN code/fingerprint, or the wallet PIN. The Bank shall not be liable for any damages arising from the unauthorised use thereof. However, the Client acknowledges that the Bank is entitled to check the legitimacy and authenticity of orders received through the use of these services.

12.11. The Client shall ensure that the funds required for the execution of their order are available at the time, including any and all fees and charges applicable to the execution of such orders at the time, which are due on their performance. If the funds on the Client's account do not fully cover such fees and charges, the Bank shall be entitled to refuse to execute the relevant order. The Bank may limit the number of orders, and the amounts involved in them, that can be placed using the K&H myID, the user name and the password, or the mobile token in a specific period of time. The Bank shall inform the User about these limits in the relevant parts of the Announcement.

12.12. The User cannot withdraw any orders given via electronic identification, except in the cases specified in these GCTC and the Announcement. The Bank shall be entitled to charge to the Client's account the amounts specified in the orders given in accordance with the GCTC during the electronic identification using the Banking Services Requiring Electronic Identification.

12.13. The Client shall be informed about the transactions performed during the use of such services in the bank account statement, or in the securities/client account statement. The Client shall immediately report to the Bank any unauthorised actions discovered in their bank account statement. However, such complaint shall not authorise the Client to delay the performance of any of its obligations to the Bank. Such complaints can be made by telephone, in writing (sent to the addresses stated in the Announcement) or in person in any branch of the Bank.

12.14. The Bank shall not be liable for any damages arising within the control of the operators or from the use of telephone lines, private switchboards and computerised systems, or the use of telephone sets or computers used by the User. Furthermore, the Bank shall not be liable for any damages arising from the use of intercepted information obtained by unauthorised access to telephone sets, telephone lines and computerised electronic systems. The User hereby irrevocably exempts the Bank from any liability that may result from a telephone conversation being cut off, repeated or distorted, or from an error in the computerised system or computer network or a disruption of their operation for whatever reason.

12.15. If the protection mechanism of the mobile device on which the mobile banking application has been downloaded and with which an active mobile token is used has been eliminated or weakened in any manner ("rooted" or "jailbroken" in particular), the Bank shall not be liable for any damages arising from frauds that were committed during the use of such a mobile device. Any and all damages arising from frauds that were committed with such a mobile device shall be borne exclusively by the User. By accepting the statement appearing when the mobile banking application is activated, the User shall acknowledge this fact and irrevocably exempts the Bank from any liability that may result from the use of such a mobile device.

13. DELETION OF THE ePIN CODE, PASSWORD, BLOCKING OF THE IDENTIFICATION DEVICE

13.1. Users shall immediately report to the Bank if they discover that

- their ePIN code, password, primary/secondary SMS password, identification device (including both the chip card and the token) and the related PIN code, password, smartphone containing their activated mobile token and their related mPIN, or wallet PIN, or the device on which the VICA application is installed and the related PIN have been lost or stolen;
- their ePIN code, password, primary/secondary SMS password, mPIN code, or the PIN code, password related to the identification device or the VICA application has fallen into the hands of unauthorised persons;
- an unauthorised transaction has been initiated using their ePIN code, password, mPIN code/fingerprint, identification device, VICA application, or wallet PIN.

13.2. Users may make such reports in writing, in any branch of the Bank or by telephone to the relevant telephone banking service; all telephone banking services can be contacted twenty-four hours a day, seven days a week with a view to the deletion of ePIN codes, passwords and mobile tokens and the associated mobile wallets,, and the blocking of identification devices or the VICA application. Such reports can only be made by Users, and the codes can only be deleted and the blocking effected by the Bank, except for mobile tokens and the associated mobile wallets, whose deletion can be initiated by the Users themselves in the e-bank or mobile bank application. The Bank will also accept such a report from another person if the relevant User is not in a position to do so and the person making the report can only assume this circumstance. In this case the person making the report must provide their personal identification details (name, address, mother's name) and assert that they are expressly requesting the deletion of the ePIN code and/or password or of the mobile token and the associated mobile wallet, or the blocking of the identification device or the VICA application. The Bank shall not examine actual authority when the report is made, and it shall not be liable for any damages arising from unauthorised reports.

13.3. The report shall include:

- If made by a natural person: the User's personal identification details (name, address, mother's name, any identification number used in banking except for a bank account number). If the User fails to comply with this requirement, the Bank may refuse to record their report and simultaneously inform the User thereof.
- If made by a legal or unincorporated entity: the details of the legal or unincorporated entity Client (name, registered office) and the User's personal identification details (name, address, mother's name, bank identification number).

When reporting such an incident – in the event of the deletion or cancellation of an ePIN code, mPIN code, wallet PIN, password, primary/secondary SMS password or identification device's or VICA application's PIN code due to the obtaining thereof by an unauthorised person – the event prompting the report must be specified together with its venue and time or, if the User does not know the exact details, its likely venue and time. If the report does not contain the User's personal identification details, the Bank may disregard it and immediately inform the User thereof. The Bank shall have the right to request further details related to the User and kept on file by the Bank in order to verify the User's authority for making such a report. The reports shall also serve as an instruction to delete the relevant ePIN code and/or password or the mobile token and the associated mobile wallet, or to block the relevant identification device or the VICA application. The Client shall be liable for any and all damage arising between the time the Client learns about the facts serving

as a basis for the report and the time when the report is made to the Bank. If the reason for the report made in order to have an ePIN code and/or password and/or mobile token and associated mobile wallet deleted or an identification device or VICA application blocked is an action assumed to being unauthorised and discovered on a bank account statement or on the account and the User does not request the deletion or blocking when making the report, the Bank shall act in accordance with the rules applicable to complaints. If a reasonably careful analysis of the facts concludes that the reported event(s) occurred in a criminal offence, the Client shall immediately report this suspicion to the relevant authorities.

13.4. Other than that, any third persons having discovered that the ePIN code, the password, the mPIN code or the telephone containing the related mobile token and the wallet PIN, or the identification device or the device equipped with the VICA application has been lost or stolen may report this in any of the manners listed in Section 13.2. Persons making such a report must give their personal details (name, address, mother's name) and the details of the identification device in question in a clearly identifiable way, and explain how they learnt about the loss or theft. If the identification device or the access via the VICA application cannot be clearly identified on the basis of the report, the Bank will disregard the report and refuse the deletion/blocking. Reports described herein shall also be governed by the other provisions of Section 13.

13.5. The local time in Hungary as measured and recorded by the central systems of the Bank shall be used to determine the time of the report as well as the time the ePIN code and/or password or the mobile token and the associated mobile wallet were deleted or the identification device or the VICA application was blocked, as well as the liability for costs, risks and damage.

13.6. Based on the report received, the Bank shall immediately proceed to implement the deletion/blocking. The deletion/blocking shall come into effect when the Bank has taken the required actions in the time needed therefor. Upon the deletion of the ePIN code and/or password all Banking Services Requiring Electronic Identification through the ePIN code and/or password shall immediately become unavailable to the User. Where a mobile token is deleted,, the token and the associated mobile wallet will be deleted only on the device(s) reported, and the mobile token and the K&H mobile wallet service may continue to be used on other devices of the same User (if any).

13.7. The Bank may charge a fee for deleting the ePIN code, the password or the mobile token, or for blocking the identification device or the VICA application. The extent of this fee is quoted in the prevailing Announcement. Such a report shall not authorise the Client to delay the performance of any of its obligations to the Bank.

13.8. The deletion of the ePIN code and/or password, and the blocking of the identification device or the VICA application shall be final and irrevocable; the ePIN code, the password, the identification device and the VICA application can no longer be used with the same registration. Deleted ePIN codes, passwords and blocked identification devices or devices equipped with the VICA application cannot be used even if they are subsequently found. The deletion of a mobile token is also irrevocable, but if the device is found, a new mobile token can be activated on it and the bankcards in the mobile wallet too can be re-digitized. The risk of deletion/blocking and any damage arising therefrom (from the fact that the deleted ePIN code/password/mobile token and associated mobile wallet, blocked identification device or VICA application cannot be used) shall be borne by the Client. The Bank shall not be liable for any damages suffered by the Client or any third parties that may result from a failure of deletion or blocking (including the unsuccessfulness of a deletion by the User for any reason falling within the interest of the User) or an abuse of their deletion/blocking. ePIN codes, passwords, mobile tokens and the digital bankcards in the associated mobile wallets, as well as identification devices can only be replaced and the VICA application used again after applying for a new ePIN code, a new password/new identification device, or activating a new mobile token for the K&H mobile banking application and re-digitizing the bankcards in the associated mobile wallet, or repeatedly requesting registration in the VICA application.

13.9. For security reasons the Bank shall have the right to delete/block the ePIN code, the password, the mobile token and the associated mobile wallet, the identification device/the identification via the VICA application if the risk arising from the relevant Contract significantly changes; if there are insufficient funds on the account, if there are reasonable grounds for suspecting that the code has been abused or misused; if the User is found to be in material breach of contract; or if the contract ceases to exist.
In addition to the above, the Bank is entitled to finally block (cancel) the physical authentication device (Token) if the User fails to renew the certificate of the identification device despite a demand to this end, within 6 (six) months from such demand.
Of the deletion/blocking the Bank shall inform the User, or in the case of a physical authentication device (Token) or VICA application the Client.

13.10. The User acknowledges that the Bank may block or delete their ePIN code, password, mobile token and associated

mobile wallet, identification device or identification via the VICA application in the following cases:

- Blocking and deletion of the ePIN code: the Bank shall block ePIN codes (for 24 hours) if it is entered incorrectly three times in succession. If an ePIN code is blocked three times within 30 calendar days, it shall be deleted finally and irrevocably.
- Blocking and deletion of the password: the Bank shall block passwords (for 24 hours) if it is entered incorrectly three times in succession. If a password is entered incorrectly five times in succession, it shall be deleted finally and irrevocably.
- Blocking of the identification device (chip card): the Bank shall block the identification device after the chip card PIN code is entered incorrectly three times in succession. The blocked chip card can only be released by the Bank and involves replacing it with a new card when the original card is handed in. The fee payable for unblocking the chip card is quoted in the relevant Announcement.
- Blocking of the identification device (Token): the Bank shall block the identification device after the Token password is entered incorrectly five times in succession. The blocked Token can only be released by the Bank after an identified phone-call to the Corporate Telephone Banking Service.
- Blocking of the mobile token: the Bank shall block the mobile token for 24 hours if the mPIN code/fingerprint is erroneously entered on the same device on three consecutive occasions. In such cases, the digital bankcards in the associated mobile wallet can still be used to authorize payments while the blocking continues. If the mPIN code/fingerprint is entered erroneously on five consecutive occasions on any device, the option of identification through the mobile token will be blocked for the User. The blocking can be released only in a branch or through TeleCenter. In that case all associated mobile wallets, including the digital bankcards therein, will be suspended.
- Blocking identification via the VICA application: the possibility of identification via the VICA application is blocked if the wrong PIN is entered on the occasion of 5 consecutive attempts while using the application. The blocking is final; the possibility of identification via the VICA application becomes accessible again only after the repeated downloading, registration and activation of the application.

14. RULES APPLICABLE TO LIABILITY FOR DAMAGE RESULTING FROM THE DELETION OF THE ePIN CODE/BLOCKING OF IDENTIFICATION DEVICES

14.1. The risk of the ePIN code, the password or the mobile token and the associated mobile wallet being deleted or the electronic identification device or VICA application being blocked, as well as of any damage arising as a result, shall be borne by the Client. The Bank shall not be liable for any damages suffered by the Client or any third parties resulting from the failure to perform the deletion or the blocking or, if otherwise permitted under these GCTC, from the failure of the deletion by the User for any reason falling within the scope of interest of the User, and from any abuse related to the deletion/blocking, or arising subsequently in connection therewith.

14.2. The Bank only accepts liability for damage arising within the control of the Client following the deletion of the ePIN code, password, mobile token and associated mobile wallet, or the blocking of the identification device or the VICA application if the damage in question is expressly attributable to the Bank's negligence. The Bank shall be exempted from liability if it successfully proves that the damages occurred due to a breach of contract wilfully committed by the User or caused by their gross negligence. Any and all risks and costs associated with electronic banking transactions or payment transactions requiring the simultaneous use of the identification device and PIN code, the VICA application and its PIN, the K&H myID and the ePIN code, the mobile token and the related mPIN code/fingerprint and the wallet PIN, and/or the user name and password and the primary/secondary SMS password shall be borne by the Client as damage arising from their wilful conduct or gross negligence.

15. AMENDMENT OF THE TERMS OF CONTRACT

15.1. The Bank shall expressly reserve and the Client shall acknowledge the right to supplement the provisions of the GCTC whenever new or improved services are introduced, and to unilaterally amend the provisions of the GCTC in force and the terms and conditions set out in the Announcement to reflect any changes in the legislation applicable or relevant to the activities and the operating conditions of the Bank; in the rulings of the Central Bank of Hungary or any other regulations binding on the Bank, the Central Bank base rate or any other Central Bank interest rates; in the opportunities for fundraising in money markets and the costs thereof; in other prime costs of the Bank, the consumer price index or state interest subsidies; in taxes and contributions, the reserve requirements or the procedures or operating processes of the Bank, and in the risk associated with a service or the Client.

Should the Bank modify the provisions of its effective General Contracting Terms and Conditions and/or relevant Announcement to the detriment of the Client, it shall be obliged to display such amended General Contracting Terms and Conditions and/or Announcement in its branches and to publish them on its website 30 days before the modification is to take effect. Should the Client not agree with such a modification, they shall have the right to terminate the contract within 30 days of the publication of the new terms, or else the modification will take effect and become applicable to the Client.

16. BANK ACCOUNT STATEMENT AND OTHER DOCUMENTS

16.1. Notices about orders given by the User in accordance with the terms and conditions of the present GCTC shall only be sent by the Bank if specifically requested by the Client. Such special notices shall be subject to a charge published in the prevailing relevant Announcements.

16.2. The document received about the service(s) used (bank account statement, special notice) shall be regarded as written proof of the execution of such orders.

17. TERMINATION OF THE CONTRACT FOR BANKING SERVICES REQUIRING ELECTRONIC IDENTIFICATION

17.1. The Contract ceases to exist:

- by extraordinary termination by the Bank with immediate effect;
- by regular termination by the Bank or the Client;
- by mutual consent on a date agreed by the Bank and the Client;
- if the Contract for all of the Banking Services Requiring Electronic Identification used by the Client ceases to exist; or
- if all bank account contracts serving as a basis for the service cease to exist for whatever reason.

17.2. In the event of a material breach of contract by the Client the Bank shall have the right to terminate the contract with immediate effect and at the same time to terminate the User's access right to the service (extraordinary termination).

17.3. The Bank has the right to terminate the Contract without an explanation, with a notice period of 30 calendar days (regular termination). The Client has the right to terminate the Contract at any time with regular termination with a notice period of 30 calendar days, provided that they have complied with all of their outstanding payment obligations.

17.4. Upon the cessation of the Contract – if a K&H e-banking service requiring chip card/token authentication is set up within the framework of the Banking Services Requiring Electronic Identification – the User shall return the identification device and the chip card reader provided by the Bank within 15 calendar days therefrom, provided that they do not use any other Banking Services Requiring Electronic Identification. Any and all damages resulting from the failure of the Client to do so shall be borne by the Client. If the User fails to return the chip card reader upon the cessation of the Contract or returns it late or damaged beyond reasonable wear and tear, they shall pay the fee of the chip card reader to the Bank. If the User fails to do so in time or at all, the Bank shall be entitled to collect the fee of the chip card immediately from the Client. The fee of the chip card reader is stated in the Announcement.

17.5. Upon the cessation of the Contract for whatever reason the access right granted to the Client and all Users under the Contract in question shall also cease to exist and consequently the Client and the Users will no longer be able to use the relevant services.

17.6. The cessation of the Contract for whatever reason shall not affect the other contract(s) of the Client with the Bank.

18. OTHER SPECIAL PROVISIONS APPLICABLE TO THE VARIOUS BANKING SERVICES REQUIRING ELECTRONIC IDENTIFICATION

For the matters concerning various Banking Services Requiring Electronic Identification not regulated in this Section, the general provisions of the GCTC shall apply.

18.1. OTHER SPECIAL PROVISIONS APPLICABLE TO K&H E-BANKING SERVICES

18.1.1. K&H e-banking services can be used by Clients who have the appropriate, valid and effective contracts for account opening and management in place with the Bank, and that have the hardware and software required for the services (see the User Manual for their list). In the case of a Joint Account as defined in the "General Contracting Terms and Conditions for Bank Account, Deposit Account and Term Deposit Products Provided to Resident and Non-resident Natural Persons", the K&H e-banking service may be used by both the natural person specified as the "Accountholder" in the bank account agreement and by the natural person specified as the "Co-Accountholder".

18.1.2. The e-bank User must have the equipment required for the use of the K&H e-banking services and specified by the Bank, and must be authorised for their use. The e-bank

User must familiarise themselves with the technical attributes of this equipment and any other tools required for the use of the services.

18.1.3. The Bank shall provide the e-bank User with physical and non-physical tools and equipment (owned by the Bank) required for the use of the services: the identification device and the chip card reader (the property of the Bank) and the installation guide demonstrating their use, as well as the banking application required for the use of the electronic identification device (mobile token) accessible in the K&H mobilbank application. The chip card reader a Bank is the property of the Bank and the e-bank User as its holder shall only be given it for use. The User Manual and the installation guide for the services and the driver for the chip card reader can be downloaded from https://www.kh.hu/ebank. The Bank reserves the right to update and supplement the User Manual from time to time in order to improve the quality of the service. The update of the User Manual shall not require the amendment of the Contract under any circumstances, and the Bank shall inform e-bank Users of such updates electronically, using the e-banking application.

18.1.4. The e-bank User may collect their identification device immediately after the signature of the Contract in any branch of the Bank. The Bank hereby points out to the e-bank User that, should it not have an identification device to give to the e-bank User for reasons beyond its control, it shall inform the e-bank User about the date by which it will be able do so when they come to collect the identification device.

18.1.5. The Bank as the owner of the driver required for the chip card reader grants non-exclusive and non-unrestricted right to the e-bank User to use the chip card reader. Only the e-bank User is authorised to use the chip card reader driver on the specified hardware and software configuration under this right for the normal use of the service, in accordance with the relevant provisions.

18.1.6. This right shall not extend to reproduction, reworking, processing and translation, including any other modifications and the reproduction of the result thereof and the preparation of backup copies.

18.1.7. The Bank hereby declares and warrants that the identification device and the chip card reader provided to the e-bank User and the driver required for the use of the chip card reader and downloadable from the Internet are free from litigation, encumbrances and claims, and no third parties have any rights that would limit the Client in exercising their own rights pertaining thereto or prevent them from doing so. The Bank hereby declares and warrants that the identification device, the chip card reader and the driver required for the chip card reader meet the specification provided by the Bank at the time of their delivery/download, and that they can be used normally on the specified hardware and software configuration.

18.1.8. The obligations of the Bank shall extend to the following:

- advice provided on the use of the identification device and the chip card reader and the installation of the driver for the chip card reader;
- troubleshooting advice;
- investigation of problem reports.

18.1.9. Furthermore, under the warranty the Bank undertakes to replace faulty identification devices and chip card readers free of charge. However, if such a fault is attributable to their abnormal use by the e-bank User, the Bank shall charge the fee quoted in the Announcement for this service.

18.1.10. The warranty provided by the Bank as per the above shall not extend to the own hardware peripherals of the Client and any software installed thereon or connected thereto; the Bank shall accept no liability for damages resulting therefrom.

18.1.11. The Bank shall not be held liable for damages attributable to malware/spyware programs outside its information technology structure. Furthermore, the Bank shall accept no liability for damages arising from a lack of proper protection (anti-virus and anti-spyware software) on the User's own information technology devices and equipment.

18.1.12. The Bank shall be entitled to use the assistance of specialist third persons in order to comply with its obligations under the warranty.

18.1.13. As a condition precedent for the warranty service, the Client undertakes to provide access to the identification device, the chip card reader, the chip card reader driver and the hardware accommodating it, and to make these available to the Bank at the conditions requested by the Bank and for the duration required for the delivery of the warranty service.

18.1.14. The validity of the identification device is visibly stated on it in a month/year format. The identification device shall be valid until 24.00 hrs on the last day of the relevant month.

18.1.15. The e-bank User shall use the chip card reader and the identification device provided by the Bank normally and

shall keep them undamaged. The Client shall immediately inform the Bank if the chip card reader gets damaged, faulty, lost or stolen, and of any other events concerning the chip card reader. The Client shall be liable for damages occurring in the chip card reader to the Bank as per the Announcement. The e-bank User shall use the chip card reader and the identification device in accordance with the installation guide provided by the Bank, and to observe the requirements set out therein.

18.1.16. The Bank reserves the right to stipulate further requirements concerning the use of the chip card reader in the relevant Announcement.

18.1.17. The identification device can only be used by the e-bank User, and it cannot be assigned, pledged as collateral or deposited as security. Legal and unincorporated entity Clients must notify the Bank when its relationship with an e-bank User as an e-bank User is terminated. E-bank Users must have their ePIN code deleted and their identification device cancelled if they have no access to other Banking Services Requiring Electronic Identification.

18.1.18. In the case of K&H corporate e-banking services the Client shall decide at their sole discretion and responsibility to which person(s) to grant an access right and what nature/content such access rights will have. Only the e-bank Users registered by the Client with the Bank according to the relevant provision and with the content corresponding to the access rights listed in the relevant Annex to the Contract shall be regarded as lawful e-bank Users by the Bank.

18.1.19. Based on the information provided by the Client, the Bank shall set up the e-bank User's access rights and manufacture the identification device to be delivered to the relevant e-bank User in person.

18.1.20. E-bank Users holding a valid identification device and entering the related PIN code, the user name and the related password, the mobile token and related mPIN code/fingerprint or K&H myID, ePIN code and primary/secondary SMS password shall have the right of disposal specified in the Contract over the accounts designated by the Client in the K&H corporate e-banking service.

18.1.21. The Client may use the relevant Annex to the Contract for notices concerning granting access rights to e-bank Users and deleting them, and modifications in user details. The Client's e-bank Users authorised thereto may do the same in the e-banking application.

18.1.22. Each e-bank User of the K&H corporate e-banking services must have at least one identification device.

18.1.23. The Bank shall enclose a PIN code to the identification device, which will be delivered to the Client in a sealed envelope. The Bank shall deliver the chip card and the PIN envelope only to the e-bank User or their Proxy. Upon receiving the chip card, the e-bank User or their Proxy shall confirm on the receipt that they have received the PIN envelope intact.
If the items are collected by the Proxy, the identification device is presented in a blocked status. The blockage may be released only when requested by the User through the TeleCenter, following identification.

18.1.24. E-bank Users are required to use both the identification device and the PIN code, or the mobile token and the related mPIN code/fingerprint, to prove their authority when exercising their right of disposal in the context of using the services.

18.1.25. The Bank shall have a new identification device manufactured prior to the expiry of the existing identification device subject to a fee.

18.1.26. When the new identification device is collected, any outstanding payments must be settled and the expiring identification device must be returned to the Bank.

18.1.27. If a technical fault occurs in an identification device, the e-bank User may apply for a replacement card. The Bank shall have the right to reject such an application without an explanation. If the technical fault of the card is attributable to improper use by the e-bank User, the Bank shall charge the fee published in the Announcement for the replacement card.

18.1.28. The Bank reserves the right to interrupt the availability of the system on an occasional basis (due to system maintenance) for short periods of time. The Bank undertakes to inform the e-bank User about the likely downtime via the system. The Bank shall accept no liability for any damages resulting from such downtimes.

18.1.29. The Bank reserves the right to interrupt the availability of the Electra system for a short period of time, due to daily system maintenance, at the time of the day and for the duration set out in the Announcement. The Bank shall accept no liability for any damages resulting from such downtimes.

18.1.30. The Bank shall send its written notices to the Client to their correspondence address/registered office specified in the Contract, and by email. The Bank shall accept no liability

for the failure of the Client to receive such written/electronic notices and the damages arising therefrom.

18.1.31. E-bank Users shall have the access rights to K&H corporate e-banking services specified in the relevant Annex to the Contract. The extent of the right of disposal granted to the different e-bank Users over the accounts involved in the K&H corporate e-banking service shall be determined by the person authorised to act on behalf of the Client under the relevant legislation. If the Contract is amended, the Parties shall monitor the access rights in force; if an inconsistency still exists, the Bank shall take into account the access rights stated in the last order.

18.1.32. **OPERATION IN PUBLIC SPACES**

In public places the e-bank User shall take care to use the chip card reader required for the service and owned by the Bank normally, keeping it undamaged. The operator and the e-bank User shall be jointly and severally liable for any damages occurring in the chip card reader on such occasions. The fee payable therefor is published in the Announcement. In public places the e-bank User shall use the chip card reader according to the installation guide provided by the Bank to the operator and to comply with the requirements set out therein.

The Bank reserves the right to stipulate further requirements concerning the use of the chip card reader by the e-bank User in public places both to the operator and the e-bank User.

The e-bank User acknowledges that the operator, pursuant to its legal relationship with the Bank, must immediately notify the Bank about any damage or fault occurring in the chip card reader or its loss, theft or any other events related thereto.

The Bank shall not be responsible for events and non-performances arising from the improper use of the chip card reader by the e-bank User.

The e-bank User acknowledges that the operator shall covenant under its legal relationship with the Bank to make every reasonable effort to identify any unauthorised uses of the services, and it shall have the system supervised by system managers twenty four hours, seven days. The Bank will not check the e-bank User's authority to use the chip card reader or the circumstances of its use. The operator shall be solely liable for any damages arising from the unauthorised use of the chip card and this liability cannot be transferred to the Bank.

The above provisions shall also apply if the e-bank User fails to use the service with the specified banking tools required.

18.1.33. **CONTRACTING USING K&H E-BANK**

Users can make contracts for using the Bank's products and services indicated in the relevant Announcements – and under the terms and conditions specified in said Announcements – also by using the K&H e-bank service. The Client Contract and all relevant documents will only be created and accepted in an electronic form in this case, and will be valid without any physical signatures.

Contracts made via the K&H e-bank become effective when the Bank makes the electronic form of the contract document (primarily, but not exclusively: contract, declaration on accepting the contract offer) available for the User in the K&H e-bank document storage area ('invoices, bankcards/documents, contracts' menu option), from where it can be accessed any time later on. The electronic document displayed in the document storage area cannot be modified later on: it can be used to check the original content of the document as recorded at the time when it was made, and to identify the declarants mentioned therein and the date and time when their declarations were made.

Following their conclusion, contracts made via the K&H e-bank can only be modified or terminated subject to the General Contracting Terms and Conditions applicable to the respective contract.

Contracts made using the K&H e-bank qualify as contracts made out in writing.

18.2. **SPECIAL PROVISIONS APPLICABLE TO K&H MOBILE BANKING SERVICES**

GENERAL PROVISIONS

18.2.1. The K&H mobile banking service is available to Users who have a valid and effective contract for K&H e-banking with the Bank and have at their disposal the hardware and software necessary for using the service. In the case of a Joint Account as defined in the "General Contracting Terms and Conditions for Bank Account, Deposit Account and Term Deposit Products Provided to Resident and Non-resident Natural Persons", the K&H mobile banking service may be used by both the natural person specified as the "Accountholder" in the bank account agreement and by the natural person specified as the "Co-Accountholder". If the User's contract for K&H e-banking services is terminated, their ability to accessing the K&H mobile banking service will also end.

LIABILITY

18.2.2. The Bank shall not be held liable for the adequacy of the Client's own hardware peripherals or of any software installed on, or connected to, the same and the Bank shall accept no liability for any and all damages arising from the above.

18.2.3. The Bank shall not be held liable for damages attributable to malware/spyware programs outside its information technology structure. Furthermore, the Bank shall accept no liability for damages arising from a lack of proper protection (anti-virus and anti-spyware software) on the User's own information technology devices and equipment.

18.2.4. The Bank maintains the right to specify further requirements concerning the use of K&H mobile banking in its relevant Announcement.

18.2.5. In mobile banking, the Client shall bear sole responsibility for which person or persons they grant an access right to for using the service and what type of access they grant with what scope. When electronic banking transactions are executed, the Bank shall consider a User a lawful mobile banking user if the Client has registered them as an e-bank user via the K&H e-banking service on condition that the access rights of a mobile bank User are the same as the access rights defined for the K&H e-bank.

18.2.6. E-bank Users having a mobile token shall have the signatory right defined in the e-banking Contract while using the K&H mobile banking service concerning the account designated by the Client as included in the K&H corporate e-banking service.

18.2.7. The Bank shall not be held liable for damage due to errors resulting from the improper use of the mobile banking Software, the improper transmission of data, wrong or incomplete data or not up-to-date information, except if demonstrably attributable to an error by the Bank.

18.2.8. The Bank shall be obliged to restore the Client's data only if such data can be proven to have been corrupted or destroyed due to a software error caused by the Bank.

18.2.9. The Bank reserves the right to interrupt the availability of the system on an occasional basis (due to system maintenance) for short periods of time. The Bank shall notify the User of the expected time of the interruption via the website and of any event that also concerns the e-bank via the e-bank system. The Bank shall accept no liability for any damages resulting from such downtimes.

18.2.10. Mobile banking Users shall have access rights to the K&H mobile banking service specified in the relevant Annex to the Contract. The extent of the right of disposal granted to the different e-bank Users over the accounts involved in the K&H corporate e-banking service shall be determined by the person authorised to act on behalf of the Client under the relevant legislation. If the Contract is amended, the Parties shall monitor the access rights in force; if an inconsistency still exists, the Bank shall take into account the access rights stated in the last order.

18.2.11. Users shall be liable themselves for damage resulting from the mobile device used for accessing the K&H mobile banking service being taken away from the User or being destroyed, failing or becoming unsuitable for any other reason whatsoever for using the K&H mobile banking service.

INSTALLATION AND DEPLOYMENT OF K&H MOBILE BANKING

18.2.12. Users shall install the K&H mobile banking service themselves, from the link stated in the relevant Announcement.

18.2.13. Those parts of the K&H mobilbank service that require User identification are accessible and may be used only after the application has been downloaded and the mobile token device has been activated. Without activation, only the functions not requiring any identification may be accessed.

K&H MOBILE BANKING SOFTWARE AUTHORISATIONS

18.2.14. Each module of the mobile banking Software is the exclusive property of the Bank. Each item in the mobile banking Software and all authorised copies of the mobile banking Software are and shall remain the property of the Bank. All intellectual property rights, copyrights, trademarks and secrets relating to the mobile banking Software are and shall remain the property of the Bank. The User has no right to sell, transfer, publish, dispose of, disclose or, in general, make available any item or any copy of the mobile banking Software to a third party unless authorised to do so by the Bank in writing.

18.2.15. The Bank grants the User the right to use the mobile banking Software, which shall be run at all times in compliance with the hardware criteria and on the operating system defined in the current Announcement. The User undertakes to use the latest version of the mobile banking Software provided to them by the Bank at all times.

18.2.16. The right to use the mobile banking Software is granted to the User on a non-exclusive basis and subject to a transfer ban. The mobile banking Software shall be used subject to the User's liability, in a manner compliant with the provisions applicable to the use of the mobile banking Software.

18.2.17. The right to use the mobile banking Software is expressly limited to the "binary code" delivered. The User shall not attempt to reconstruct the "source" of the mobile banking Software or to perform reconstruction from any other component of the Software (by way of disassembly, decompilation or in any other manner).

18.2.18. The User shall not have the right to modify the mobile banking Software or to combine it with other Software, unless expressly authorised to do so. If such an authorisation exists, then the User shall bear all and any risk arising from such a modification, with special regard to the risk of incompatibility between the modified mobile banking Software and any hardware, software or future software, software version, software update, test, diagnostic or control routine.

18.3. **TERMS OF USE OF THE K&H MOBILE WALLET**

18.3.1. The K&H mobile wallet service will be accessible to K&H mobile bank Users who, as Card Holders, have at least one K&H bankcard as specified in the Announcement, in accordance with these GCTC. To be able to take advantage of the service, Users as above are required to accept the terms of use of the K&H mobile wallet.

18.3.2. K&H mobile wallet functionalities requiring electronic identification are only accessible after K&H mobile bank sign-in and identification.

18.3.3. Mobile payment is based on communication between the User's mobile device and the POS terminal when the device is brought near the POS terminal.

18.3.4. To be able to execute mobile payments with digital bankcards the NFC (Near Field Communication) function on the mobile device used needs to be switched on.

18.3.5. Payments can be executed with mobile devices in offline mode (i.e. without internet connection) subject to the terms and conditions set forth in the Announcement.

18.3.6. For the K&H mobile wallet service, the Bank may stipulate more demanding technical parameters than those for the K&H mobile bank. The operating system required for and other technical parameters with respect to the K&H mobile wallet service are specified in the Announcement as effective.

18.3.7. In addition to the provisions set forth in this section, use of the K&H mobile wallet service is governed by the rules applicable to the K&H mobile bank.

18.4. **SPECIAL PROVISIONS APPLICABLE TO K&H TELECENTER SERVICES**

18.4.1. The K&H Telecenter is provided to natural persons using the Bank's banking services.

18.4.2. Transactions executed via the K&H Telecenter and their fees shall be governed by the provisions published in the Announcements concerning the bank accounts, deposit accounts and term deposits of natural persons and concerning investment services and securities dealings.

18.5. **SPECIAL PROVISIONS APPLICABLE TO THE K&H CÉGVONAL SERVICE**

18.5.1. The K&H Cégvonal telephone banking service is provided with the banking services specified in the General Contracting Terms and Conditions for the Bank's account management, deposit and lending services to businesses.

18.5.2. Clients may specify or modify the access rights of their authorised Transacting Persons in the relevant Annex to the Contract.

18.5.3. Each Querying/Transacting Person can query all the accounts of the Client without restrictions or limitations. However, transaction orders can only be given by Transacting Persons authorised by the Client.

18.5.4. A Transacting Person can modify or terminate their own authorisation to use Banking Services Requiring Electronic Identification by phoning K&H Cégvonal to register this request.

18.5.5. The termination of a Transacting Person's authorisation to use Banking Services Requiring Electronic Identification may be requested by the Transacting Person themselves (by telephone or in writing) or by the Client. The Client may exercise this right only by registering the request in writing with a branch administrator. The Transacting Person's instructions shall be accepted by the Bank until the day on which the Client registers the request.

18.5.6. If the Client terminates all the authorisations of all the Transacting Persons, then only the Client shall be authorised to act, via a branch administrator, until the new Transacting Person(s) are appointed.

18.5.7. The Transacting Person shall not have the right:

- to transfer to others their right to dispose over an account included in the scope of the Banking Services Requiring Electronic Identification;
- to collect bank account statements or
- to sign, amend or terminate contracts for services outside the scope of Banking Services Requiring Electronic Identification.

18.5.8. No Transacting Person role can be given after November 2, 2016. Instead of this role, the rights of disposal defined in Chapter III. Services and Annex 11 of the Announcement for Corporate Clients can be given to Users specified after November 2, 2016.

18.6. **SPECIAL PROVISIONS APPLICABLE TO THE K&H CORPORATE CUSTOMER SERVICE**

18.6.1. The K&H Corporate Customer Service is a service provided by the Bank to Clients that are resident or non-resident legal or unincorporated entities, organisations (foundations, churches, associations, municipalities etc.), businesses or private individuals engaging in commercial activities by telephone whose scope is determined in the prevailing Announcement and particularly includes the provision of information and general help, complaint management and advice concerning the corporate products of the Bank as well as taking instructions.

18.6.2. The ePIN code may be deleted at the express request of its holder and in the cases defined in Section 12.4.

18.6.3. The termination of a Telephone Representative's access rights may be initiated by the Telephone Representative themselves (by telephone or in writing) or by the Client. The Client shall exercise this right only in writing, via its relationship manager. The instructions of the Telephone Representative shall be accepted by the Bank until the day on which the Client terminates their access right, after which only the Client shall be authorised to act, via its relationship manager, until a new Telephone Representative is appointed.

18.6.4. No Telephone Representative powers can be given after November 2, 2016. Instead of this role, the rights of disposal defined in Chapter III. Services and Annex 11 of the Announcement for Corporate Clients can be given to Users specified after November 2, 2016.

18.7. **SPECIAL PROVISIONS APPLICABLE TO ELECTRA SERVICES AND K&H ELECTRA24 ELECTRONIC BANKING SERVICE BASED ON A MOBILE PHONE APPLICATION**

GENERAL PROVISIONS

18.7.1. Under the Electra service (hereinafter: the Service), the Electra User may take the following actions electronically in the currency defined in the Announcement:

a. submit orders and notifications to the Bank,

b. perform bank account statement queries of their account balance and turnover,

c. gain access to the current day foreign currency/FX exchange rates of the Bank and the FX exchange rates of the National Bank of Hungary.

d. if a separate agreement exists to this effect, the user can manage the accounts kept at other banks in line with the provisions regulating the service.

18.7.2. The Electra User may perform Electronic Banking Operations for the execution of which the submission of documents by the Client or a third person and the inspection of the documents by the Bank or a third person are necessary pursuant to the Contract or legal regulations, only if having fulfilled these obligations in advance.

18.7.3. For the purposes of Electronic Banking Operations performed by Electra Users, the time established by the computer system of the Bank shall be regarded as the time of receipt of the order or the notification by the Bank.

18.7.4. In its Announcements, the Bank may publish limitations on the scope and the amount of Electronic Banking Operations.

18.7.5. The Bank may allow Electra Users to perform additional Electronic Banking Operations in the future. The Bank shall notify Electra Users of such changes.

18.7.6. The Bank provides Electra Users with Forms for the purpose of written notifications relating to the Service. The Bank shall accept written communications by Electra Users to the Bank as valid only if submitted on these Forms.

18.7.7. Certain sub-services provided to Electra Users by the Bank under the Service (e.g.: installation, error fixes) may also involve third-party experts.

18.7.8. The bank charges for the Service are published in the relevant Announcement of the Bank. Should the Contract stipulate bank charges different from the ones defined in the Announcement, the rates defined in the Contract shall apply.

18.7.9. The Bank shall also notify Electra Users directly through the Electra System of any changes if the Service or any condition relating to the Service justify such notification or if the Electra User and the Bank so agreed in this regard.

18.7.10. THE SPECIAL FEATURES OF THE SERVICE

A detailed description of the basic and supplementary services is published in the latest, prevailing Announcement.

ELECTRA INSTALLATION AND DEPLOYMENT

18.7.11. Clients themselves shall install the Electra service accessible on fat clients, using the installation toolkit, which can be downloaded from the Bank's website, and an installation code sent to the Client by SMS, with the help of the group code, user name and Token specified in the data sheet. Otherwise, if the Client specifically requests administration by the Bank or requests help from the Bank having opted for administration by the Client, the Electra service is installed by the Bank at the site specified by the Client for a fee defined in the Announcement. If the service is installed by it, the Bank shall also provide training on the use of the installed system. The Client shall sign the Installation Report to confirm that the Bank has installed the Electra Software in compliance with the Contract.

18.7.12. The Electra service available via web interface (webElectra) can be accessed from any computer that meets the requirements as defined in the Announcement, having Internet connection. No software is to be installed for using the service; however, in the case of identification device physically linked to the computer (e.g. a token) the driver and the browser pug-in of that device must be installed. The Bank may determine the browsers that can be used for the service.

ACCESS RIGHTS:

18.7.13. The Client registers with the Bank the authorised persons in the relevant Annex, along with the scope of their access rights to the Electra service.

In the case of administration by the Client, the access rights may cover the following:

a) query right specified for each account,

b) right to record transactions specified for each account.

c) query right for all accounts,

d) signatory right specified for each account,

e) group right defined per identifier.

f) self administration right – administration of user access rights, except for the signatory right over the account

g) executive right – administration of user access rights, including the signatory rights over the account.

The above listed rights can be set on the interface enabling administration by the Client or they can be set by the Bank. Exceptions to this are the executive rights, which can only be set by the Bank, upon the written request of the persons authorised to sign on behalf of the company.

The Bank is entitled to charge a fee as determined in the Announcement for any setting performed by it.

18.7.14. Electra Users having query or other rights shall gain access to the items for which they are authorised after providing their Token passwords or if using webElectra, via the VICA application.

18.7.15. Electra Users having query rights for all accounts may perform queries of every account of the Client. The scope of this query right automatically extends to newly opened accounts, for which the query right of the User shall be granted automatically. To modify rights, Clients themselves shall set the appropriate authorisations if Client side administration is opted for. In the case of administration by the Bank, Clients shall request the necessary authorisations for the new account in a data sheet.

18.7.16. Signatory rights shall be defined for each User with the help of a score (of 1 to 10 points). The Bank shall only accept the orders signed with 10-point authorisation. For the submission of orders, signatory rights defined for specific accounts have to be defined in the case of current accounts. A non-account specific signatory right shall be required at the time of the software installation in order to register the client program and also for the termination of term deposits, for the confirmation of authorisations relating to direct debits and, in the case of Client side administration, for the registration of additional users.

18.7.17. The Client shall bear responsibility for the choice of the person or persons whom they authorise to use the Electra System installed at the Client. The Bank and the Electra

System shall regard as authorised the persons who have been registered by the Client in the case of Client side administration or who have been reported to the Bank as such in the form provided by the Bank in the relevant Annex. The user authorisation levels specified this way shall only apply to the Electra client terminal.

18.7.18. The Bank shall set centrally:

a) in the case of Client side administration: the authorisations of the first two Users.

b) in the case of Bank side administration: the authorisations of the Users specified by the Client.

The User shall set their Token password at the time of the first registration. In the case of Users having signatory rights, the same code will qualify as the code required for the approval, confirmation of specific orders.

18.7.19. The Electra User shall ensure that no other person has access to their Token password. The Bank shall not be liable for damages arising from unauthorised use.

18.7.20. The User shall accept that if they enter their Token password incorrectly for five times in succession, they shall automatically lose access to the Electra service thereafter.

18.7.21. In the event defined in Section 18.7.20., the User shall release the blocked Token password themselves by contacting the Bank's telephone customer service; the ePIN code will be required.

18.7.22. The Client shall notify and consult the Bank in advance if they intend to modify their hardware or software system.

RECEIPT AND EXECUTION OF ORDERS

18.7.23. The deadlines for the receipt by the Bank of the Orders and the deadline for the execution thereof are specified in the Announcement.

18.7.24. It is the Client's/User's own responsibility to make regular back-ups of the computer files containing their orders and notices. If the Electra program installed on the Client's computer is damaged, the Bank can only guarantee the retrieval of the saved data.

18.7.25. The Bank shall regard as valid orders only those orders that were submitted to it by the User, were found formally correct by the Electra System and, in terms of content, fully complied with the provisions of legal regulations and of the Contract.

18.7.26. The Bank shall be entitled to debit the account in accordance with the orders that were signed using the Token or the VICA application.

MODULE FOR MANAGING ACCOUNTS KEPT AT OTHER BANKS

18.7.27. The Client becomes entitled to use the module for managing accounts kept at other banks within the webElectra service based on a separate agreement concluded with the Bank. The Bank shall provide the services enabling the management of accounts kept at other banks based on the provisions defined herein, as well as in the relevant agreement concluded with the Client and the Announcement, which provisions may differ from the ones set forth in the general terms and conditions defined for the webElectra service. The 'Management of accounts held in other banks' module can only be used subject to identification with a Token ID device or via the VICA application.

18.7.28. The management of accounts kept at other banks is possible in Hungarian and in English.

18.7.29. The Electra User becomes entitled to perform the following operations as part of the module for managing accounts kept at other banks:

a) initiate transfer orders with manual data entry,

b) initiate transfer orders with file import,

c) conversion between domestic and international file formats,

d) generate reports for balance and client data and account statements,

e) administration of user rights (self-administration).

18.7.30. Within the module for managing accounts kept at other banks, the following orders may be initiated: transfers within the company group, transfers to third parties, lump sum transfers (wage transfers). The orders may be generated individually or based on a template, from a file or via file import from the Client's ERP software (file import).

18.7.31. Within the module for managing accounts kept at other banks, the Electra User may view and/or print (day-end, mid-day) account statements, may initiate detailed transaction searches, query value dated balances, and may export the account information into various file formats.

18.7.32. The Electra User may revoke the orders given in the module for managing accounts kept at other banks until the order has been duly signed. Thereafter the Bank's

relationship manager should be contacted to revoke the order. If the Electra User wishes to revoke a payment order to be executed from or to a bank account kept at the Bank, provided that the order's currency is Euro or the currency of a member state of the EEA outside of the Euro zone and that the bank of the paying party and of the beneficiary has its principle place of business in one of the member states of the EEA, the following provisions shall apply:

a) The payment order may no longer be revoked once the Bank has received it. A payment order shall be deemed received by the Bank when it has been signed and sent to the Bank.

b) A value dated order may be revoked until the end of the banking day preceding the agreed date of debiting at the latest.

18.7.33. The Banks shall define the time of execution based on the order's time of receipt (verified by digital signature, in a condition suitable to be accepted).

SPECIAL PROVISIONS PERTAINING TO K&H ELECTRA24 ELECTRONIC BANKING SERVICE BASED ON A MOBILE PHONE APPLICATION

18.7.34. K&H Electra24 electronic banking service based on a mobile phone application may be used by Clients who are entitled to using the webElectra service. K&H Electra24 electronic banking service based on a mobile phone application may only be used together with the VICA application only. The Bank provides K&H Electra24 electronic banking service based on a mobile phone application upon receipt of the Client's application to this end and the conclusion of the contract, subject to the prices stipulated in the current Announcement.

18.7.35. Logging onto K&H Electra24 electronic banking service based on a mobile phone application, and the approval of banking transactions available in the application and requiring electronic identification shall take place using K&H's myID, subject to identification via the VICA application. If the Electra User chooses so, the application allows the system to remember the K&H myID linked to the User in question.

18.7.36. As part of K&H Electra24 electronic banking service based on a mobile phone application, Electra Users become entitled to use the services and function requiring electronic identification and execute transactions, as set out in the Announcement.

18.7.37. K&H Electra24 electronic banking service based on a mobile phone application is available in Hungarian and English. The technical conditions of using this service are stipulated in the current Announcement.

18.7.38. The user rights of Electra Users in respect of K&H Electra24 electronic banking service based on a mobile phone application, are identical to the scope of user rights pertaining to using the webElectra service.

18.7.39. Otherwise, K&H Electra24electronic banking service based on a mobile phone application, is governed by the stipulations pertaining to the webElectra service, subject to the exceptions described in the present section.

BLOCKING; THE REPORTING OBLIGATION OF USERS

18.7.40. Blocking, in the case of Client side administration, is performed by the Client (or other User) themselves with the help of the Electra terminal or by phone with the help of the Bank using the ePIN code.

18.7.41. In the case of Bank side administration: The User shall report the following events immediately upon being informed of them by calling the phone number defined in the Contract (available 24 hours a day, every day of the year):

a. access by unauthorised persons to the Token Password, and

b. loss or theft of the Token

c. the device on which the VICA application is installed is no longer in the possession of the Electra User (lost or stolen) and the PIN of the application is accessed by an unauthorised person.

d. an unauthorised operation in the Client's bank account statement, due to which the Client requests (in the case of the Electra Software) the blocking of the Service or the blocking of any User.

18.7.42. The reporting of the above listed events must contain the Client's company name, registered seat, tax number, account number, the accurate definition of the event reported, the name of the reporting person and a fax/phone number at which the Bank can confirm the reported event as well as a declaration that the reporting person expressly requests, in the case of the Electra Software, the blocking of the entire Service or a specific User. If the reporting person does not request blocking at the time of reporting the event, the Bank shall proceed in accordance with the rules pertaining to complaints.

18.7.43. The Bank shall execute blocking immediately during the phone-call in the case of events reported between 7.00 AM and 5.00 PM on banking days. In the case of events reported on holidays and between 5.00 PM and 7.00 AM on banking days, the Bank shall execute the blocking before the processing of the payment items received after 5.00 PM on the previous banking day.

18.7.44. Within one hour of the blocking but on the next banking day at the latest, the Bank shall confirm the event reported and the blocking by sending a fax message to the fax number specified by the reporting person.

18.7.45. An event is considered reported if the reporting person has provided all of the data requested by the Bank (with the exception of only the tax number). The blocking shall become effective when the Bank has taken the measures required for the blocking within a reasonable time necessary these measures. The Bank shall record the time of reporting in accordance with the local time applied in the Bank's systems.

18.7.46. The Client shall bear the risk of blocking and all damages arising from the fact that the blocked Token password cannot be used. The Bank shall assume no liability for damages suffered by either the User or by any third person due to the failure to block the Token password or the abuse of the blocking process.

18.7.47. If the damage arising from unauthorised use was not caused by the intentional behaviour or gross negligence of the User, the User shall cover the damage arising before the reporting and the request for the blocking of the Token password up to a cap of HUF 45,000.

18.7.48. The Bank shall keep a record of the events reported. Upon the request of the Client, the Bank shall issue a certificate of the fact that an event was reported and on the content and time of the report made retroactively for a period of maximum five years.

18.7.49. Any damages arising between the time of being informed of the fact forming the basis of the reporting and the time of reporting of this fact to the Bank shall be borne by the Client.

18.7.50. The Bank shall be liable for the damages arising after the reporting of the relevant event unless the damage arising after reporting is caused by the User themselves by an intentional or grossly negligent breach of contract.

18.7.51. If a judgment of the facts with the generally expected care suggests that a criminal act has taken place, the Client (or other User) shall immediately report this suspicion to the authority competent for the investigation of criminal acts.

18.7.52. The blocking of the Token password is final and irrevocable. The Service may not be used from the time of confirmation until the release of blocking. The blocking may be released by the representative of the Client personally at the account managing branch by filling out the Form received at the branch and signing it in the corporate signature registered with the Bank.

18.7.53. The costs arising at the Bank and at the Client in relation to the blocking shall be borne by the Client.

LIABILITY

18.7.54. The Bank shall not be liable for the damages arising from errors in the Electra Software, the inappropriate transmission of data, incorrect or incomplete data or non-updated information unless such damages can be proven to have occurred due to an error of the Bank. Also, the Bank reserves the right to interrupt the availability of the system on an occasional basis (due to system maintenance) for a short time. The Bank shall notify the Electra User via the system of the expected time of the interruption. The Bank shall not be liable for damages potentially arising from such interruptions.

18.7.55. The Bank shall be obliged to restore the Client's data only if such data can be proven to have been corrupted or destroyed due to a software error caused by the Bank provided that the Client took measures to ensure that the data can be restored from materials stored in a format readable by the Electra System.

18.7.56. The Client shall cover all damages arising from the inappropriate use of the Tokens provided to the Users or the use of the Tokens by an unauthorised person, as well as all damages resulting from the use, by an unauthorised person, of the mobile device used for the purpose of accessing K&H Electra24 electronic banking service based on a mobile phone application. The only exemption from this rule shall be the damages arising after the reporting of the Token; or, in the case of the Electra Software, the Service; or, in the case of K&H Electra24 electronic banking service based on a mobile phone application, the blocking of the application, to the Bank.

18.7.57. The Client shall be liable before the Bank and other collaborators for all damages arising from the fact that the orders placed by the User or the data provided by the user were inappropriate, incorrect or incomplete.

18.7.58. The Bank shall not be liable for damages arising from the fact that the instruction (order) of the User is damaged, becomes unintelligible or is accessed by unauthorised persons during data transmission due to the faulty operation or the failure of the modem or the data connection. The Bank shall have no liability for damages arising from the manipulation of the data files by any person during data transmission.

18.7.59. The User shall use the Electra Software at the risk and liability of the Client and may connect the computer/mobile device to the Bank's Electra System at the liability of the Client. Accordingly, the Bank shall not be held liable on the grounds of damage to the Client's computer/mobile device or the data files stored on the Client's computer or damage to other peripherals, computers, mobile devices, software or data files connected to the Client's computer caused by the Electra Software or the Electra System or an error or breakdown of the Electra Software or the Electra System or any other damage arising from the fact that the Client is not authorised to dispose over the computer appointed for the installation of the Electra Software.

ELECTRA SOFTWARE AUTHORISATIONS

18.7.60. Each module of the Electra Software is the exclusive property of the licensor of the Bank and each item of the Electra Software and each authorised copy made of the Electra Software is and shall remain the property of the licensor of the Bank. All intellectual property rights, copyrights, trademarks and secrets relating to the Electra Software are and shall remain the property of the Bank and the licensor of the Bank. The Client (User) has no right to sell, transfer, publish, dispose of, disclose or, in general, make available any item or any copy of the Electra Software to third parties unless authorised to do so by the Bank in writing.

18.7.61. The Bank grants the Client or the User the right to use the Electra Software, which shall be run at all times in compliance with the hardware criteria and on the operating system defined in this GCTC. The Client shall always use the latest version of the Electra Software provided by the Bank, which shall either be updated online or the current updates may be downloaded from the Bank's Internet portal and installed on the Client's computer.

18.7.62. The right to use the Electra Software is granted to the Client on a non-exclusive basis and subject to a transfer ban. The Electra Software shall be used under the Client's exclusive liability, in a manner compliant with the provisions applicable to the use of the Electra Software.

18.7.63. The right to use the Electra Software is expressly limited to the "binary code" delivered. The Client shall not attempt to reconstruct the "source" of the Electra Software or to perform reconstruction from any other component of the Electra Software (by way of disassembly, decompilation or in any other manner).

18.7.64. The Client shall not have the right to take a backup of the Electra Software. The Client has no right to modify the Electra Software, to combine it with other software unless expressly authorised to do so. If such an authorisation exists, the Client shall bear all and any risk arising from such a modification, with special regard to the risk of incompatibility between the modified Electra Software and any hardware, software or future software, software version, software update, test, diagnostic or control routine.

18.7.65. The Bank shall grant the right of use for a period starting on the day of delivery of the Electra Software and ending when the Client terminates the use of the Service or the Contract concluded between the Parties terminates for any other reason.

18.7.66. If the Client fails to comply with any of the obligations defined in the Contract regarding the use of the Electra Software, the Bank shall be entitled to immediately withdraw the right of use in respect of each item of the Electra Software without any special legal procedure.

18.7.67. The Client shall take all necessary measures in order to protect the rights of the Bank or the licensor of the Bank from violations by the Client's own employees and representatives or any other person who may have access to the documentation, the Electra Software and the know-how.

18.7.68. If failing to comply with the above obligation, the Client shall bear full liability for all legal consequences and for the breach of the Contract including the obligation to indemnify for the damage caused.

18.7.69. The Client shall destruct the Electra Software within one day of the day of termination of their right of use for any reason and send a written declaration to the Bank of the destruction of the software.

ELECTRA SOFTWARE WARRANTY

18.7.70. The Bank warrants that the Electra Software complies with the specifications communicated by the Bank at the time of delivery and that it can be used properly on the contractual hardware and operating system. In the case of installation by the Bank, the Bank shall install the Electra

System and train, in a maximum of 2 hours, one person acting on behalf of the Client to use the Electra System at the site of installation.

18.7.71. The warranty of the Bank shall not extend to the peripherals of the hardware containing the Electra Software and any hardware and software connected to the Electra Software.

18.7.72. The Client acknowledges that the Bank may use the services of third-party experts for the installation of the Electra Software and the fulfilment of its obligations under the warranty.

18.7.73. The warranty service of the Electra Software covers the following:

a. advisory service in relation to the installation of the Electra Software Module, the updates and corrections provided and authorised by the Bank,

b. advisory service for the identification of errors,

c. advisory service for the solution of the problems arising during the installation of the updates and corrections,

d. temporary fixes and alternative solutions,

e. investigation of reports on problems,

f. delivery of updates.

18.7.74. As a precondition for the provision of the Electra Software warranty service, the Client undertakes to provide access to the Electra Software and the hardware containing the Electra Software under the conditions requested by the Bank and for the time required to provide the warranty service during the entire term of the Contract. The Client shall always use the latest Electra Software version provided by the Bank.

18.7.75. Services beyond the scope of the Electra Software warranty:

a. solving problems arising from non-contractual or non-documented use of the Electra Software or negligence,

b. regenerating the Electra Software in the cases when regeneration is necessary due to an error not attributable to the Bank,

c. modification of the functions of the Electra Software upon the Client's request.

TERMINATION OF SERVICE

18.7.76. If the Client does not use any Electra Software Module (does not log on to the Electra client program) for a period of at least 12 months, the Bank may delete the Electra Software Module not used from the Electra System. If the Client does not use the Electra Software Module (or, in the case of more than one Electra Software Modules, all of the modules) for more than 18 months, the Bank may terminate further access of the Client to the Electra System, which shall imply automatic termination of the Contract.

18.7.77. In the case of termination of the Contract for any reason, the fees, commissions and charges not paid to the Bank shall become due and payable in a lump sum on the day of termination.

18.8. **SPECIAL PROVISIONS APPLICABLE TO K&H E-POST SERVICES**

18.8.1. The K&H e-post service is available to the Users of the non-natural-person Clients that have a valid and effective contract in place with the Bank for the products defined in the relevant Announcement and have the hardware and software required for the use of the service, as are listed in the user manual.

18.8.2. In the case of K&H e-post services requested and accounts opened after November 2, 2016, the Client shall forgo receiving paper-format account statements, through Magyar Posta Zrt. (Hungarian Post) or otherwise, with respect to all existing and future payment accounts and securities accounts. Any condition deviating from this may be included in a unique contract. In the case of Contracts concluded prior to November 2, 2016, the terms and conditions of the K&H e-post service – with regard to the already existing accounts – are contained in the already concluded contract.

18.8.3. The e-post User must have, and be authorised to use, the equipment defined by the Bank as necessary for the use of the K&H e-post service. E-post Users shall familiarize themselves with the technical attributes and the proper use of these equipment and other tools necessary for the use of the service. The Bank shall not assume liability for damages arising from improper use.

18.8.4. If so requested, the Bank shall provide the e-post User with the physical and non-physical devices (identification device and chip card reader) as required for the use of the services (the property of the Bank), and the installation guide demonstrating their use, as well as the Bank's application enabling the use of the electronic

identification device (mobile token) available for the users of the K&H Mobile Bank application. The user manual and the installation guide for the services and the driver for the chip card reader can be downloaded from https://www.kh.hu/ebank. The Bank reserves the right to update and supplement the user manual from time to time in order to improve the quality of the service and develop the applications. The update of the user manual shall not constitute an amendment of the Contract under any circumstances, and the Bank shall inform e-post Users thereof electronically through the Internet using the e-post application.

18.8.5. Regarding the definition of access rights in the case of the K&H e-post service, it is the Client's exclusive responsibility to determine the person or persons who are authorised to use the service. For the purpose of the execution of electronic banking operations, the Bank shall regard those persons as legitimate e-post Users who have been reported to the Bank as such on the form provided by the Bank in the relevant Annex.

18.8.6. The Bank sets e-post User authorisations on the basis of the authorisations reported by the Bank and produces the identification devices to be provided personally to the given e-post Users.

18.8.7. The Client may request from the Bank the cancellation of the access rights of a certain e-post User or the modification of user data in writing on the form provided the relevant Annex.

18.8.8. The Bank reserves the right to interrupt the availability of the system on an occasional basis (due to system maintenance) for a short time. The Bank shall notify the e-post User of the expected time of the interruption. The Bank shall not be liable for damages potentially arising from such interruptions.