COMMERZBANK

ERSTE Bank

Electronic Banking Services
General Terms and Conditions

as amended in a consolidated form

with respect to the transfer of the portfolio of deposits and framework agreements for financial services under Section 17 of Act CCXXXVII of 2013 between Commerzbank Zrt. (Transferor) and ERSTE Bank Hungary Zrt. (Transferee)

Effective date of the amendment: 1 December 2022

The detailed information on the amended provisions is included in the Customer Notice sent to Corporate Customers dated on 31 August 2022.

1. Effect of the General Terms and Conditions

1.1.   The effect of these General Terms of Contract (hereinafter the "**GTC**") shall extend to all electronic banking services provided in relation to payment bank accounts opened and kept for the Account Holder through the Electronic Banking System (hereinafter the "**Service**").

1.2.   The provisions of the GTC shall be binding on both the Account Holder and the Bank.

1.3.   If in relation to the Service there is a issue not provided for in the Contract or these GTC, the provisions the Business Rules, General Terms and Conditions of Payment Services and the Announcement and the relevant laws shall prevail.

1.4.   The Bank shall display these GTC, the Business Rules and the Announcement in its customer services premises, make them available on the Bank's website (until 30 November 2022 at www.commerzbank.hu, from 1 December 2022 at www.erstebank.hu), and shall make them available free of charge at any time during the term of the agreement upon the Account Holder's request.

1.5.   In the event of any discrepancy between the GTC and the Business Rules, the provisions of these GTC, or in the event of a discrepancy between these GTC and the Contract, the provisions of the Contract, or in the event of a discrepancy between these GTC and the Announcement, the provisions of the Announcement, in the event of a discrepancy between the Announcement and the Contract, the provisions of the Contract shall prevail.

1.6.   **The Bank shall provide payment and deposit services under these GTC only to an Account Holder who has a Contract with Commerzbank on the date of entry into force of these GTC. The Bank shall not enter into any new Contract subject to these GTC.**

2. Definitions and Interpretation

API Channel: an electronic channel of the Electronic Banking System that provides indirect, secure communication that enables the Corporate Customer to access all Bank Accounts accessible through the Erste Electra Program indirectly through the application of a Third Party Provider (TPP) registered with the National Bank of Hungary or the European Banking Authority.

Bank: **until 30 November 2022: Commerzbank Zrt.** (registered seat: 1054 Budapest, Széchenyi rakpart 8., company registration number: Court of Registration of the Metropolitan Tribunal of Budapest: 01-10-042115, activity licence number: State Bank Supervisory Authority Decision No. 20/1993 (case no.:01257/1993.) **from 01 December 2022: Erste Bank Hungary Zrt.** (registered seat: H- 1138 Budapest, Népfürdő u. 24-26, Court of Registration of the Metropolitan Tribunal of Budapest: 01-10-041054; tax identification number: 10197879-4-44; group identification number: 17781042-5-44, group community tax number: HU17781042; activity licence number and date: I-2061/2004 of 26 August 2004).

Commerzbank's Electra Software, (from 01 December 2022, the Archive Electra Software), the software called Electra, which contains the client-side software of the Electronic Banking System and which provides users with the ability to perform Electronic Banking operations, and which software will be transferred to Erste Bank as of 30 November 2022.

Electra ID (also as User Name/ID or VICA User ID): data used for the identification of User(s) for login into the Electronic Banking System.

Electronic Banking System: a payment system that allows remote access, via a computer, for Electronic Banking operations, through which the Account Holder can submit payment orders to the Bank and perform other operations, in particular, viewing and downloading account information. Use by the Account Holder of the Commerzbank Electra Software and the Erste Electra Program provided by the Electronic Banking System.

Electronic Banking Software: the software comprising the client-side program of the Electronic Banking System provided by the Bank to the Account Holder (Commerzbank Electra Software (from 01 December 2022 Archive Electra Software) and the Erste Electra Program), which provides the possibility for authorised users to perform Electronic Banking transactions.
.

Erste Electra Program (thick client): the client-side program of the **Electronic Banking System** installed on a personal computer required for use of the Erste Electra Program Service and all separately ordered and activated Program Functions that enable Users to perform Electronic Banking operations. The Bank guarantees the trouble-free provision of the Erste Electra program only when the latest version is used. The Bank places the latest version of the type of the Erste Electra Program for mandatory download on its website or it can be downloaded from the relevant menu item of the Erste Electra Program. The Erste Electra Program can manage up to 999 (nine hundred ninety-nine) Accounts and 255 (two hundred fifty-five) Users.

Strong Customer Authentication – „SCA": an authentication based on the use of two or more elements
a)   categorised as knowledge (something only the customer knows);
b)   possession (something only the customer possesses); and
c)   biological property (something the user has)
that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data. The Bank applies Strong Customer Authentication from 14 September 2019.

Other Electronic Banking Channels (SWIFT): communication channels providing access to the Electronic Banking System, where the Bank does not provide client-side Electronic Banking Software. **Electronic Banking Channels providing EBICS and host-to-host connectivity will be discontinued on 1 December 2022.**

Individual (non-batch) order: an order for a single payment transaction submitted individually by a User through the Electronic Banking System.

User: fully identified private individual who may use the Electronic Banking System with the rights specified in the Contract.

User name: an identifying name for the identification of the User.

Global Payment Plus (GPP): **to be discontinued on 1 December 2022.**

Third Party Provider (TPP): a common name for the Payment Initiation Service Provider (PISP), the Account Information Service Provider (AISP) and the Card Based Payment Instrument Issuer (CBPII).

User Guide: information available on the "?" icon in the Erste Electra Program, which provides a detailed description of the technical features of using the Electra Program.

Announcement: the List of Conditions for Corporate Customers received from Commerzbank through a portfolio transfer.

Micro-Business: Corporate Customers defined as microenterprises under Section 2 (17) of the Payment Services Act.

Order Package: a batch created by the User for simultaneous signing of one or more transaction and sending them together to the Electronic Banking System, in which the time of forwarding and receipt of all individual orders sent to and received by the Bank shall be deemed identical compared to each other.

photoTAN signature: the signature solution used in the GPP application, which will be phased out on 1 December 2022 in view of the discontinuation of the GPP application.

SMS Code: a time-limited one-time password to a given user in a message (hereinafter the SMS Code): a one-time, time-limited series of digits sent to the phone number provided in the User Data Form for the use of the VICA application and/or SMS login/signature which is intended to identify the User. The SMS Code is sent by the Bank by SMS with a time limit of 5 minutes. After the time limit has expired, the SMS Code cannot be used for the purpose it was sent. An SMS Code is sent for the following purpose:
- **to authenticate the User's VICA registration;**

Personalised Security Credentials: personalised features provided to or generated by the User for the purposes of the identification of the Account Holder and authentication of the orders placed by it (e.g. User Password, User Name, Electra Group Code, Electra ID, SMS Code, VICA User ID, VICA Password, VICA Registration Code).

Contract: an individual contract concluded by and between Commerzbank and the Account Holder with respect to the

.

Electronic Banking Software of which these GTC, the Bank's Business Rules in effect from time to time, the General Terms and Conditions of Payment Services and Deposits and the Announcement form an integral part. The Contract shall apply to the use of both the Commerzbank Electra Software (Archive Electra Software) and the Erste Electra Program from the date of entry into force of these GTC.

Installation Manual: a document forming a part of the installation kit of the Erste Electra Program, which contains instructions for its installation.

Customer Notice: Annex Electronic Banking Service GTC to the customer notice on portfolio transfer dated on or about 30 August 2022.

Business Rules: the Business Rules for financial and ancillary financial services for customers transferred from Commerzbank Zrt. to Erste Bank Hungary Zrt. in the framework of a portfolio transfer pursuant to Section 17 of the Banking Act.

General Terms and Conditions for Corporate Payment Services and Deposits: the terms and conditions of Commerzbank Zrt. for Corporate Customers (Micro-Businesses and Consumers) with respect to financial services and the General Terms and Conditions of Contracts of Deposits as amended in a consolidated fo rm the effect of which extends to the Corporate Customer with framework agreements for payment services and deposit contracts transferring from Commerzbank Zrt. to Erste Bank Hungary Zrt. in the framework of a portfolio transfer pursuant to Section 17 of the Banking Act.

Corporate Customer or Account Holder: a customer of Commerzbank Zrt. that qualifies as an enterprise or micro-business whose payment services framework agreement is transferred to Erste Bank by way of portfolio transfer.

VICA Application: a mobile application that can be installed on a smartphone operating on Android and iOS operating systems, providing a secure and independent communication channel between the User and the Bank without the use of any additional authentication device to log into or confirm or reject signing through the Erste Electra System during the use of VICA.

VICA Password: the password created by the User upon registration of the VICA Application, which the User shall provide each time when he/she opens the VICA Application.

VICA User ID: identification data provided by the Bank to the User which the Account Holder provides for the registration of the VICA Application.

VICA Registration Code: one-time Personalised Security Credentials provided by the Bank to the User which the Bank sends by SMS to the mobile phone number specified by the User in the Contract and which the User gives when registering the VICA Application.

3. General Provisions

3.1.   The use of the Service is subject to a valid bank account agreement between the Account Holder and the Bank, the Contract(s) with respect to the Service and the minimum hardware and software requirements in force at any given time. The minimum IT and software requirements shall be governed by the hardware and software conditions set out in Annex 1 to these GTC as at the date of entry into force of these GTC. The Bank shall notify the Account Holder of any changes to the minimum requirements set out in Annex 1 (e.g. the release of a new software version and the mandatory installation and use by the Account Holder) via the Erste Electra Program. The new terms and conditions shall apply without any amendment to Annex 1, as of the date specified in the notice of amendment. In the event of an update of the Erste Electra Program, the User Guide for this new version shall prevail.

3.2.   Within the framework of the Service, the Account Holder may submit to the Bank orders related to the Services specified in the Contract and in these GTC and may request lists and extracts thereof.

3.3.   Using the Electronic Banking System, the Account Holder may generate an electronic account statement of the payment transactions executed in the bank accounts included in the System. The Account Holder acknowledges that, irrespective of the above, only the account statement provided by the Bank on paper (sent by post) shall be deemed authentic. The information sent by and printed from the Electronic Banking System shall be for information purposes only. The Bank shall continue to send the Account Holder an account statement for transactions carried out with the Electronic Banking System as provided for in the relevant bank account agreement or the General Terms and Conditions for Payment Services with the content, manner and frequency as required therein. In addition, the Account Holder may request information on his/her current bank account balance, completed daily transactions and pending items for a fee.

3.4.   The Bank is entitled to engage the services of a professional third party for the provision of certain services (e.g. installation, troubleshooting, warranty) within the framework of the Electronic Banking System.

.

3.5. **The Bank is entitled to offer to the Account Holder, instead of the electronic signature method(s) specified in the individual contracts, another, more secure electronic signature solution or, in case of mandatory industry parameters, to require the Account Holder, which the Account Holder accepts upon the terms and conditions offered by the Bank.**

4. Operation of the Electronic Banking System

4.1.   The Bank shall process orders forwarded with error-free content and in appropriate form) to and received by it through the Electronic Banking System and carry out the tasks related to performance within its competence in accordance with the payment service and other laws, the General Terms of Contract on each Service, in compliance with the Notice in effect from time to time.

4.2.   The Account Holder shall ensure that the IT and telecommunication devices required for the use of the Electronic Banking System specified in the GTC are available and that the scope of User rights are defined and their Personalised Security Credentials are confidentially managed and updated at regular intervals, modifications are reported to the Bank and its IT and telecommunication devices are continuously protected and are safe.

4.3.   The Bank warrants that the Electronic Banking Software and the Erste Electra Program can be used for their intended purpose if the IT - hardware and operation systems specified in these GTC exist. The Bank's warranty does not apply to the Account Holder's IT devices and peripheries and other software running on its IT equipment.

4.4.   During the use of the Electronic Banking System, the Account Holder is obliged to fully comply with the requirements (especially the GTC, the Security Rules, the User Guide, technical, hardware and software requirements) and also have its Users comply with them in full. The Account Holder shall be liable for all damage caused by the failure to follow the provisions or instructions concerning Users.

4.5.   The Bank's IT system environment logs the Order (Package)s sent to the Electronic Banking System. The Account Holder accepts the validity of data recorded in the Bank's Electronic Banking System and, in the case of any dispute that may arise, recognises it as evidence in respect of both the placement and execution of Order (Package)s. The Account Holder accepts that the time recorded by the Bank's IT system shall be considered as the time of the arrival of an Order (Package) at the Bank through the Electronic Banking System.

4.6.   When installing the Electronic Banking Software and Erste Electra Program, the User shall change the Login Password provided by the Bank at the first login and create his/her own Login Password.

4.7.   During the use of the Electronic Banking System, the Account Holder shall be obliged to fully comply with and cause the Users to comply with the user instructions and User Guide provided. The Account Holder shall bear any damage resulting from the failure to comply with the user instructions, User Guide.

4.8.   The Service is available 24 hours a day, 7 days a week. The Account Holder acknowledges that the Electronic Banking Service may be suspended for the time being during the period of maintenance of the Electronic Banking System on the Bank's side. The Bank shall carry out the maintenance after the cut-off times for each type of transaction in such a way that it does not impede the execution of the orders submitted for that day.

5. Electronic Banking Services

5.1.   Archive Electra Software Electronic Banking System

The Electra Group Code, Electra ID, User Password, VICA ID required to log in the Archive Electra Software Electronic Banking System and to retrieve a Bank Statement will remain unchanged.

No new Order (Package) can be entered in the Archive Electra Software Electronic Banking System, from which only information can be requested on Orders recorded before the entry into force of these GTC as follows:

5.1.1.   Basic services of Electra Light version (can be installed on one workstation only)
- Provision of Electronic Account Statement
- Querying executed daily transactions
- Querying account history
- Exporting and importing data in specified formats

5.1.2.   Basic services of Electra Business version (networked version)

- Provision of Electronic Account Statement
- Querying executed daily transactions

.

- Querying account history
- Exporting and importing data in specified formats

- Encrypted data transfer between the Bank and the Account Holder
- Receipt of DETSTA and STATUS reports received up to migration

5.1.3. Electra service version
- Services according to Section 5.1.2, and
- Receipt of DETSTA and STATUS reports received pending migration

5.1.4. Global Payment Plus application - to be discontinued as of 1 December 2022.

5.2. Erste Electra Program

5.2.1. The Account Holder shall install the Erste Electra Program for the use of the Erste Electra Program Service for which the installation kit may be downloaded from the website of the Bank (www.erstebank.hu). The "**Electra Group Code**" and "**Electra Identifier**" indicated in the Contract can be used in the Erste Electra Program without any changes, Erste Bank Hungary Zrt must be accepted in the VICA application. The Bank shall send the VICA registration password to the respective User to the telephone number specified in the Contract.

5.2.2. The Account Holder undertakes to install and put in operation the given version of the Erste Electra Program on its computer or computer network in accordance with the relevant Installation Manual. The Bank undertakes to install the Erste Electra Program upon the request of the Account Holder.

5.2.3. The User shall change his/her Login Password generated by the Bank once the Erste Electra Program is installed when he/she first logs in. If the User fails to change his/her User Password, the Erste Electra System warns the User to change his/her password until the User changes it. When handling his/her User Password, the User shall proceed pursuant to the provisions of the Security Rules on the condition that the User is permitted to log in even if the User Password is not changed.

5.2.4. The Order (Package) entered into the Erste Electra Program and login are authorised in the VICA Application.

5.3. Access (User) rights in the Erste Electra Program

5.3.1. The Account Holder shall give the names of its Users, by completing the relevant form. The Account Holder may grant Users the following User rights:
   (i)   Signature Right
   (ii)   Right to Query
   (iii)   Right to Sign on Behalf of a Company
   (iv)   Collective Right

5.3.2. The Account Holder has assigned to the holders of User Rights at the time of the entry into force of these GTC the number of points for the User Rights specified above in the Contract, which shall remain valid without any change in the Erste Electra Program. User Rights to be granted after the entry into force of these GTC may be notified to the Bank with the help of the form used by the Bank.

5.3.3. The Bank shall execute the Order Package(s) if they are signed by a User or Users who individually or collectively have at least 10 Signature Points for the given Order type.

5.3.4. The transactions that may be executed in the Erste Electra Program with each User Right are set out in Annex 2 to these GTC.

5.3.5. Users designated by the Account Holder in the Contract as having the Signature Right or the Right to Query shall automatically be granted all the entitlements associated with the Signature Right and the Right to Query as set out in Annex 2 to the GTC by the Bank in the Erste Electra Program as of the date of entry into force of these GTC.

5.3.6. Users authorised by the Account Holder in the Contract with the "Company Administrative Signature Right" and/or "Deposit Right" shall automatically be granted all entitlements associated with the "Company

Signature Right" as set out in Annex 2 to the GTC by the Bank in the Erste Electra Program as of the date of entry into force of these GTC.

5.3.7. The Users authorised by the Account Holder in the Contract with "Collective Right" shall automatically be granted all powers within the "Collective Right" set out in Annex 2 of the GTC by the Bank in the Erste Electra Programme as of the date of entry into force of these GTC.

5.3.8.   The Bank shall allow using the Electronic Banking System only to the Users whose identification has been carried out in accordance with the Act on the Prevention and Combating of Money Laundering and Terrorist Financing and the Bank's relevant Business Rules. The Account Holder is responsible for which persons he/she grants User Rights through the Electronic Banking System.

5.3.9.   The User may log in to the Electronic Banking System by entering the VICA Password and using the VICA application, which meets the requirements for Strong Client Authentication, given that logging in to the Electronic Banking System is done using two independent categories of elements - knowledge and possession.

5.3.10.   The Bank expressly draws the Account Holder's attention to the fact that the register of Users recorded in the Electronic Banking System is independent of the persons who are authorised to give instructions in respect of the Account Holder's accounts on paper and who are registered in the signature card. The Bank will not automatically delete a person deleted from the signature card from the list of persons entitled to use the Electronic Banking System, and vice versa. Accordingly, the Account Holder shall be solely responsible for the notification or deletion of the persons notified on the signature card or having access under the Electronic Banking System.

5.3.11.   The Account Holder and the User may use the Electronic Banking System only in accordance with the rules set out in these GTC, the Security Rules and the User Guide. The Account Holder and its Users are obliged to take all measures that are generally expected in the given situation to ensure that the Electronic Banking System and other devices required for its use, in particular the Erste Electra Program and data and passwords that constitute Personalised Security Credentials, as well as the mobile device containing the VICA application are kept safe by the User and are not accessible to unauthorised persons.

5.3.12.   The User shall not record or store any data or passwords that constitute Personalised Security Credentials.

5.3.13.   It is the Account Holder's duty and responsibility to ensure the protection of client-side information, to set, maintain and protect passwords, Personalised Security Credentials, to monitor access to data and protect it against unauthorised use, to make, store and manage backups of such data and to perform all other tasks related to data security and confidentiality.

5.3.14.   Any breach of these security and prevention obligations in relation to these GTC shall be deemed to be intentional or grossly negligent conduct of the Account Holder or the User. The Bank shall not investigate the right of the user of these Personalised Security Credentials to use them and the circumstances of their use, and the Account Holder shall be liable for any damage resulting from the unauthorised use of the Personalised Security Credentials by third parties as set out in these GTC.

5.4. Access to the Electra API Channel

5.4.1.   The Bank shall set the API Channel access right for the Users designated by the Account Holder upon the Account Holder's request. The Bank opens the Electra API Channel for the following types of TPPs.

5.4.2.   Payment Initiation Service Provider (hereinafter the "PISP")

The Account Holder may also submit payment orders to the Bank through the API channel via PISP. If the Account Holder initiates the execution of a payment transaction through PISP, the Bank shall inform the Account Holder of the following:

(i)   the Bank meets the requirements of the Payment Services Act to have a secure connection for data transmission with the payment service provider providing the payment initiation service,

(ii)   immediately upon receipt of the payment order, the Bank shall inform PISP fully of the initiation of the payment transaction and shall make available to the payment service provider providing the payment initiation service the information available for the execution of the payment transaction, which may be shared with the Account Holder,

.

(iii)   it manages payment orders issued directly by the Account Holder and made with the use of the payment initiation service in the same way, in particular with regard to timing, order of execution and fees.

In Annex 2 of these GTC the Bank lists the services which it makes available to PISPs.

5.4.3.   Account Information Service Provider (hereinafter the "AISP")

If the Account Holder uses an Account Information Service provided by an AISP, the Bank shall inform the Account Holder of the following:

(i)   the Bank has a safe connection for data transmission with the AISP,

(ii)   Ii manages requests for information transmitted through the various account information services provided by the AISP and initiated through the direct bank channel without discrimination .

In Annex 2 of these GTC the Bank lists the services which it makes available to AISPs.

If the Account Holder allows access to the account through the AISP for the use of the Account Information Service, then simultaneously the Account Holder expressly consents to the AISP being able to independently initiate access to the Account Holder's account in the absence of the Account Holder, up to four times per day per query type within 24 hours permitted by law.

The Bank makes the following query types available to AISPs for account access without the presence of the Account Holder:

(i) bank account balance query,

(ii) query of account history of the past not more than 90 days.

5.4.4.   Card Based Payment Instrument Issuer (CBPII)

In order to be able to use the CBPII service, the Account Holder shall have the Erste NetBank service. The Account Holder is entitled to associate the Card Based Payment Instrument issued by a CBPII with any of its Bank Accounts available through Erste NetBank. One Card Based Payment Instrument may be assigned to one Bank Account. During the assignment, the Account Holder expressly consents to the Bank performing the CBPII's request. The Account Holder acknowledges that a given CBPII is entitled to request confirmation from the Bank until the Card Based Payment Instrument and the assignment of the Bank Account are not terminated or the respective CBPII or Bank Account is not blocked.

Upon the CBPII's request the Bank shall confirm without delay whether the funds needed to execute the card based payment transaction are available on the Bank Account of the Account Holder.

Conditions for the Bank's confirmation:
(i) the payment account is available online when the query is made,
(ii) the Account Holder expressly consents to the Bank performing the CBPII's request,
(iii) the consent of the Account Holder is available before the first confirmation is requested.

Requirement for the CBPII's request for confirmation:
(i) The Account Holder expressly consented to the request for confirmation,
(ii) The Account Holder initiated the card based payment transaction with a cash based payment instrument issued by the CBPII,
(iii) CBPII identifies itself with the Bank each time before requesting a confirmation.

The Bank's response to a CBPII's request for confirmation may only be "yes" or "no". Regardless of the answer to the query, the Bank is not entitled to block funds on the payment account.
The Account Holder is entitled to request information from the Bank on the name of the payment service provider requesting confirmation and the content of the confirmation. The Account Holder shall reach that information in the NetBank among the data indicated in the "Logbook".

When a TPP service is used, the Bank shall indicate the scope of data transferred to TPP, the purpose and legal basis of the data transfer to the TPP in the case of Account Holders who are private entrepreneurs and primary producers, in its Data Processing Notice available at www.erstebank.hu/en/adatkezelesi and at any branch office of the Bank.

Orders received through the API Channel will be charged at the same rates as Orders submitted through the Erste
.

Electra Program or NetBank. The Final Cut-off Times applicable to the submission of payment orders are the same as Final Cut-off Times of Orders submitted through the Erste Electra Program or NetBank.

The Bank may deny access to the Bank Account via PISP or AISP in the following cases:
For objectively justified and duly substantiated reasons related to AISP's or PISP's unauthorised or fraudulent access, including initiating an unauthorised payment transaction or initiating a payment transaction fraudulently. The Bank shall inform the Account Holder in writing prior to the denial of access but not later than after denial of access and the reasons for denial. The Bank shall not be obliged to provide information if the information is inappropriate for objectively justified security reasons or if the obligation to provide information is prohibited by law. Once the reason for denying access has ceased, the Bank shall re-grant access.
The Bank shall immediately inform the Supervisory Authority of any denial of access, the relevant details of the case and the reasons for such denial. The Supervisory Authority shall evaluate the case and take appropriate action as necessary.

5.5. RECEIPT AND EXECUTION OF ORDERS (PAYMENT ORDERS) IN THE ERSTE ELECTRA PROGRAM

5.5.1. **Signing Order (Packages)**:
Order (packages) sent to the Bank through the Erste Electra Program shall be authenticated and signed by the User having Signatory Right by the User giving the VICA Password and signing the Order (Package) in the VICA Application.

The authentication and signing of the Order (Package) as per the above meets the requirements of strong customer authentication as the authentication and signing of the Order (Package) happens with the application of two components falling into categories independent of each other - knowledge and possession.

5.5.2. The Bank shall consider the Orders signed by Users having Signatory Right as per the above and sent to the Bank **as a (payment) order authorised by the Account Holder**.

5.5.3. The Bank shall execute the **Order** received through the Erste Electra Program in accordance with the these GTC and the Announcement.

5.5.4. The Order (Package) shall be deemed to have been received by the Bank if it communicates the fact and time of receipt of the Order (Package) in a message (confirmation) sent by the Electronic Electra Program. The fact of receipt does not guarantee the execution of the Order (Package). If several Orders are sent to the Bank in the form of a Package and there are no sufficient funds to execute all Orders, the Bank attempts to process Orders in the order in which they were sent to the Bank in the Electronic Banking System provided that the Bank reserves the right to process and execute Orders that are part of an Order Package in any order.

5.5.5. In the case of Orders which encounter a technical problem while they are entered in, and thus the receipt of the Order is not confirmed, the Bank shall be entitled to consider the Order as not submitted to the Bank (not received by the Bank).

5.5.6. The User is entitled to submit several Orders (Packages) from login to the Erste Electra Program until exit. In this case, the Bank sends a message through the Electronic Banking System about the receipt of the Order Packages that are sent to the Bank simultaneously.

5.5.7. The Electronic Banking System stores the status of Orders received and confirmed by the Bank. The Account Holder may query the status of the submitted Orders from the Erste Electra Program. In addition, the Bank shall notify the Account Holder of rejection in the manner specified in the account contract of the Account Holder entered into with respect to the Account affected by the rejected Order.

5.5.8. When a given Service is used, payment orders received through the Erste Electra Program are accepted and processed by the Bank with the same content requirements as applicable to paper orders. The Account Holder and the User acknowledge that orders sent to the Electronic Banking System may be withdrawn, cancelled or modified in accordance with the GTC on Corporate Payment Services and Deposits. The Bank shall be entitled to refuse to execute orders containing incompliant, incomplete, incorrect or otherwise inadequate information in accordance with the applicable laws and regulations and the terms and conditions of the Account Contract affected by the order.

5.5.9. If the balance on the Account Holder's Account is not sufficient for the execution of the orders at the time when they would be executed – including the amount of fees and expenses to be charged for the execution of the Orders which are due and payable when the Orders are given – the Bank shall refuse to execute the Orders immediately in accordance with the provisions of the account contract of the Account concerned, or, if they are queued for the period in accordance with the Announcement, the Bank refuses execution after the period of queuing expires.
.

5.5.10. The Bank shall not send the User of the Account Holder further notice through the Erste Electra Program of the fact that the payment order is queued. The Bank shall notify the Account Holder of queuing as specified in the account contract of the Account Holder entered into with respect to the Account affected by the queued Order.

5.5.11. The Bank shall accept Orders for execution on the same day up to the Final Cut-off Time specified in the Announcement in effect from time to time in respect of each Order type.

5.5.12. The Bank shall process value-dated transfer orders and transfer orders between one's own sub-accounts that may be placed in the Electronic Banking System under the following rules:

If they relate to the same day or a past date are submitted after the cut-off time (save for VIBER orders which, if the value date is given, shall be deemed to be submitted for execution on the relevant date, then transfer orders and/or transfer orders between own one's sub-accounts given with the indication of the debit date or start date of processing shall be processed on the following Banking Day which will be the actual date of processing.

5.7.13. If a transfer order cannot be executed for reasons beyond the Bank's control, the Bank shall notify the Account Holder in the manner specified in the account contract of the Account concerned.

6. NOTIFICATION OBLIGATION, LIABILITY AND DEACTIVATION

6.1. The Account Holder and the User may use the Electronic Banking System only in accordance with the rules set out in these GTC, the Security Rules and the User Guide. The Account Holder and its Users are obliged to take all measures that are normally expected in the given situation to ensure that the Electronic Banking System and other devices necessary for its use, in particular the Archive Electra Software and the Erste Electra Program, as well as data and passwords that constitute Personalised Security Credentials and the mobile device containing the VICA application are kept secure by the User and are not accessible to unauthorised persons.

6.2. The User shall not record or store any data or passwords that constitute Personalised Security Credentials.

6.3. It is the Account Holder's obligation and responsibility to ensure the protection of information on the customer's side, set, maintain and protect passwords, Personalised Security Credentials, monitor data access and protect them against unauthorised use, back up, store, manage and perform any other task related to data security and protection of confidentiality.

6.4. For the purposes of these GTC, the Account Holder or the User is deemed to act intentionally or with gross negligence if he/she breaches this security and prevention obligation. The Bank shall not investigate the right of the User to use these IDs and the circumstances of their use, and the Account Holder shall be liable for any damage arising from the unauthorised use of the ID by third parties as provided for in these GTC.

6.5. Both the Account Holder and the User shall act as generally expected in the given situation when using the Electronic Banking System, therefore they shall especially immediately notify the Bank and initiate the deactivation of the User Right of a User when they become aware of the following:
   (i) its/his/her devices by which it/he/she accesses to the Electronic Banking System (in particular, its/his/her computer(s) and (business administration and corporate management system) are no longer in its/his/her possession (within its/his/her control) or there is a chance of an unauthorised third party gaining access to them;
   (ii) its/his/her Personalised Security Credentials required for the use of the Electronic Banking System Service and for identification and the smart phone/SIM card that belongs to the phone number reported for the receipt of the SMS Code, smart phone/SIM card containing the VICA application are no longer in its/his/her possession (within its/his/her control) or there is a chance of an unauthorised third party gaining access to them;
   (iii) there is an unauthorised (payment) order (transaction) in its/his/her account statement;
   (iv) an unauthorised (payment) order has been initiated through the Electronic Banking System.

6.6. The Account Holder may give notice and initiate deactivation of Access right by phone each day of the week, round the clock (0-24 h), through Erste Corporate TeleBank on 06 1 298 0223, furthermore in written notice by email to erste@erstebank.hu, or the Bank's central mailing address (H-1138 Budapest, Népfürdő utca 24-26., Hungary) and in person in writing during the opening hours of the customer service in any Branch Office or in the Company Office.

.

Once given, no notice may be withdrawn. The notice shall contain the identification data of the person giving the notice, the Account Holder's name, the account number, a description of event that provides a base for the notice and its place and time, the transactions concerned. After notification was made by phone, the Bank may ask a written confirmation from the Account Holder.

6.7.   The notice shall be deemed ineffective if the notifier cannot be identified, the account number is given incorrectly or the content of the notice and the circumstances of notification arouse the suspicion that it is false. The Bank disclaims any liability for any legal consequences or damage arising out of an ineffective notice. In order to verify the identity the person giving notice, the Bank is entitled to request further data, however the Bank shall not examine the identity of the person giving notice before cancellation.

6.8.   After notice has been given, the Bank immediately deactivates the Electronic Banking System. The system cannot be used until the Banking Day that follows the receipt by the Bank of the written request that the Person with Signatory Right submits in person for the reactivation of the Electronic Banking System.

6.9.   The Account Holder shall not be liable for any unauthorised payment transaction if:
(i) it could not detect before the execution of the payment transaction that the circumstances described in Section 6.5 have arisen,
(ii) the damage was caused by an act or omission of an employee of the Bank, a payment services intermediary, a branch or an entity carrying out an activity outsourced by the Bank,
(iii) the Bank did not require strong customer authentication,
(iv) the damage was caused by a personalised procedure which qualifies as a payment instrument, with the use of an IT or telecommunication device, or without the use of personalised security features such as the identification codes used by the Account Holder or its Users,
(v) the Bank did not enable the Account Holder to give notice or request cancellation.

6.10.   After notice is given, the Bank shall have liability for any damage related to unauthorised payment orders that were placed with codes stolen from or removed from the possession of the Account Holder or the User that were used on the User's side of the Erste Electra System or any damage resulting from unauthorised use of the Electronic Banking System.

6.11.   The Bank shall be released from liability if it proves that damage related to an unauthorised payment order was caused by the Account Holder or its User acting fraudulently, or such damage was caused by intentional or grossly negligent breach of their obligations concerning the safe use of the Electronic Banking System set forth in these GTC and the Contract and its annexes, furthermore, in any case where it proves that the breach has been caused by a circumstance beyond its control, unforeseeable at the date of conclusion of the contract, and it could not avoid the circumstance or avert the damage with due care.

6.12.   For the purposes of these GTC, the Account Holder/User shall in particular be deemed to **act intentionally or with gross negligence**:
(i) pro-active behaviour or omission of the Account Holder or its User which is in conflict with the performance of its/his/her obligation to comply with these GTC, the Contract, the User's Guide, the Installation Manual and the Security Rules to safely and properly use the Electronic Banking System – including without limitation to store and keep in confidence the Personalised Security Credentials, the mobile phone/SIM card registered for the receipt of the SMS Code, the mobile phone/SIM card belonging to the VICA Application and any other identification data – as a result of which the Account Holder or the Bank suffers or might suffer damage,
(ii) making available or accessible or permitting any authorised third party to use or become familiar with the Electronic Banking Software in any way,
(iii) if the Personalised Security Credentials, the mobile phone/SIM card registered for the receipt of the SMS Code, the mobile phone/SIM card belonging to the VICA Application are kept in the same place as technical devices necessary for the operation of the Electronic Banking System in a way that makes them accessible to unauthorised persons,
(iv) the technical devices needed for the operation of the Electronic Banking System, the computer on which the Electronic Banking Software has been installed or through which it is used and the Personalised Security Credentials are stolen or removed by an unauthorised person if this results from intentional conduct or gross negligence of the Account Holder or any User, especially if this results from that the premises or device where this equipment, software, Personalised Security Credentials are kept are left unattended or the protection of their security is insufficient,
(v) the failure to meet or fully meet or any delay in meeting the notification/cancellation obligation,
(vi) breach of any requirement set forth in the GTC, the Security Rules, the User's Guide or the Installation Manual concerning the safe and proper use of the Electronic Banking System.

.

The Bank is entitled to file a criminal report in the event of the acquisition of the Personal Identification Data by an unauthorised person or misuse of the Personal Identification Data.

6.13.   The Account Holder acknowledges that if the User Password, the VICA Password is unsuccessfully entered three (3) times consecutively, the Erste Electra System shall automatically deactivate the User.

6.14.   The removal of a User's deactivation may be initiated in writing by the Account Holder submitting the written form standardised by the Bank for this purpose (with authorised signature and by submitting appropriate proof for the right of representation).

6.15.   If the User forgets his/her VICA password, the VICA application needs to be reinstalled, for which the Account Holder may request a new VICA Registration Code from the Bank, any other Personalised Security Credentials necessary for the use of a VICA Application remain unchanged. The Bank will charge a fee for providing a new VICA Registration Code for the reinstallation of the VICA application.

6.16.   By submitting a form standardised by the Bank for this purpose, the Account Holder may initiate in writing that in respect of a User
   (i)   a new Login Password should be generated for his/her entry in the Electronic Banking System which is sent by SMS to the User when he/she is present in a Bank Network Unit to the telephone number that is indicated in the User Data Form as the place to send the Signature Password; or
   (ii) a new Login Password should be generated for his/her entry in the Electronic Banking System which is sent by SMS to the User.

6.17.   After 5 minutes the SMS code becomes invalid, so the User must initiate the transaction again.

6.18.   The Bank may also initiate the deactivation of the User Rights of a given User in the relevant Electronic Banking System if it suspects fraudulent circumstances, misuse, unauthorised or illegal use, informing the Account Holder to that effect. Immediately after deactivation the Bank shall notify the Account Holder in writing or by SMS of the fact and reasons of deactivation, unless compliance with the notification obligation jeopardises the Bank's security or is prohibited by law. The given User's Access Right may only be re-activated after consultation with the Account Holder and with the Account Holder's written consent. The Bank disclaim any liability for any damage that may be incurred by the Account Holder as a result of deactivation.

6.19.   Any expenses incurred by the Bank and the Account Holder in relation to deactivation shall be borne by the Account Holder.

6.20.   After deactivation, the Service may be used following reactivation. The Account Holder may request reactivation in writing in the form standardised by the Bank for this purpose in the account servicing Company Office.

6.21.   The Account Holder shall require the User to change his/her Personalised Security Credentials upon reactivation. If the User does not initiate a change, the former Personalised Security Credentials remain valid. The Bank shall not accept any liability for any damage resulting from this.

6.22.   The Users of the Account Holder may only use the Electronic Banking System at the Account Holder's risk and liability and connect to the Bank's Electronic Banking System their computers/mobile devices or telecommunications systems that are used for login to the Electronic Banking System at the risk of the Account Holder. The Bank shall have no liability for any damage resulting from inappropriate, unprofessional or unauthorised use of the Electronic Banking System or technical defects or disruptions arising within the control of the Account Holder and the resulting loss of data, inadequate transmission of data or malfunctioning of lines.

6.23.   The Bank shall have no liability for any damage suffered by the Account Holder resulting from any of the above or the failure to execute any payment order that is filled in erroneously or is incomplete or is impossible to be executed. The Bank shall have no liability for any damage caused by the failure to notify the Bank about changes in the identity of Users authorised to use the Electronic Banking System or their User Rights.

6.24.   The Bank shall deem a User's User Right valid as long as the Account Holder does not change the given User's User Right by notifying the Bank as required to that effect, i.e. only by completing, signing and submitting to the Bank the relevant User Data Form with the indication of the change or deletion. The Bank shall take steps to register the change immediately when it receives and confirms the User Data Form during opening hours in any Bank Network Unit or, but not later than on the Banking Day of receipt. Regarding this the Account Holder may exercise its right to give notification or instructions if the person(s) acting on behalf of the Account Holder evidence(s) his/her/their

appointment (mandate) and gives credible evidence of his/her/their signature, and the detailed of rules of evidencing are governed by the provisions of the relevant Bank Account Contract.

6.25.　　The Bank shall ensure compliance with the data protection and data security laws, however for the operational safety and confidentiality of the Electronic Banking System the Bank shall only accept liability to the extent of the liability borne by other service providers participating in operating the system (e.g. telephone company or internet service provider) regarding their own systems. The Bank shall not accept any liability for any damage resulting from this.

6.26.　　The Account Holder shall have full liability for damages suffered by the Bank as a result of damage to the Electronic Banking System, its unauthorised use or permitting unauthorised persons to use it, its tampering or copying the Electronic Banking Software in relation with the Contract.

6.27.　　The Account Holder and its Users shall have exclusive and full liability towards the Bank for the accuracy of the data contained in the orders forwarded to the Electronic Banking System.

6.28.　　The Account Holder shall have liability for all damage caused by all general malicious codes or similar malicious programs or program parts which are proven to have reached the Bank with the intermediation of the Account Holder.

6.29.　　After the installation of the Electronic Banking System, the Electronic Banking System configuration files may only be altered subject to prior consultation with the Bank. The Bank shall not accept any liability for any damage caused by alterations carried out without such consultation and shall charge the Account Holder for the costs of debugging.

6.30.　　The Account Holder shall be liable for any loss of data that may arise during the receipt of the Orders (Order Packages) sent to the Bank or damage arising out of Orders sent to the Bank with data that does not conform to the data required by the rules on the completion of (payment) orders as long as the Account Holder does not receive a confirmation of receipt of the Order from the Bank. Thereafter the Bank shall be liable for any damage caused by non-execution of Orders because of loss of data or inappropriate content. The Account Holder is obliged to check the execution of its orders on the basis of the account statement of the Account.

6.31.　　The Bank shall keep records on the notices under Section 6.5 which shall function as a reliable and unalterable proof for the dates and contents of notices for at least 18 (eighteen) months. At request of the Account Holder (or a person authorised by the Account Holder), the Bank shall provide a certificate about the date and content of notices free of charge, but only once for each notice. The Bank shall issue the certificate of notices given during the past one year within 15 business days and, within 30 business days, of notices given earlier than the past one year.

6.32.　　The Account Holder and its Users shall use the Electronic Banking System properly for its intended purpose and in compliance with the provisions of these GTC, the Security Rules, the User's Guide. The Account Holder shall be liable for all damage caused by the failure to follow the provisions or security rules set out in the above documents.

6.33.　　The Account Holder and its Users shall only initiate communication with the Electronic Banking System from a computer that they know and regard as reliable which meets the following security requirements at least:
  (i)　　has appropriately configured and maintained, up-to-date anti-virus and firewall software in operation,
  (ii)　　the security updates of the operating system, browser and anti-virus and firewall software used on the computer have been installed,
  (iii)　　the software programs running on it are known to and safe for the User as an operating environment.

6.34.　　For the secure use of the Electronic Banking System, the Account Holder ensures that
  (i)　　daily updated and regularly run antivirus and antispyware software is installed on the computer running the Electronic Banking System;
  (ii)　　the computer running the Electronic Banking System is separated from the local area network with a client-side firewall, and only the firewall rules necessary and sufficient for the communication of the Electronic Banking System are implemented on the firewall in the operating system running the Electronic Banking System;
  (iii)　　only registered Users have access to using the Electronic Banking System;
  (iv)　　the Users' Login Passwords are complex (2 numerals, lower case letters, upper case letters, at least 8-character long) and are modified on a monthly basis;
  (v)　　the automatic updating of the operating system is activated or security updates are installed at least every week and refrains from:

.

a)   having shared files on the computer running the Electronic Banking System which contain the installation and data storage folder of the Electronic Banking System;

b)   granting system administrator rights to the Users on the computer running the Electronic Banking Software with respect to its operating system;

c)   switching on the logging of accessed files for the installation and data storage folder of the Electronic Banking Software and saving and keeping such logs.

6.35.   The Bank only warrants the provision of the Electronic Banking Program Service if the latest version of the given type of the Erste Electra Program is installed. The Account Holder may check which version of the program is currently in use, under the menu item "Setting Parameters/Settings/Program updates" of the Erste Electra Program, and it can also download the latest version of the given program type.

6.36.   The Bank warrants that the Erste Electra System can be used properly for its intended purpose if the above mentioned technical devices are available and the latest version of the program type of the Erste Electra Program is used.

7. Copyright

7.1.   The Account Holder is granted a non-exclusive and non-transferable licence to use the Electronic Banking System, without transferring the relevant copyright and other intellectual property rights. Apart from this licence, the Account Holder is not entitled either to adapt, develop, sell or permit any third parties to use or otherwise dispose of all or any part of the Electronic Banking System. In addition, all copyright and other intellectual property rights related to the Electronic Banking Software are vested in the Bank and the Bank's licensor as exclusive proprietor.

7.2.   The Account Holder may not make any copy of the Electronic Banking Program, reverse engineer, disassemble its source code and to interconnect it to any other software without licence. If the Account Holder is given permission to interconnect the Electronic Banking System with other software, the Account Holder shall bear all risks originating from such interconnection (e.g. loss of data).

8. TERMINATION OR EXPIRY OF THE AGREEMENT

8.1. Contracts are made for an indefinite period. The Contract terminates:
- (i) by ordinary notice,
- (ii) with immediate effect (by extraordinary termination) whether by the Bank or the Account Holder,
- (iii) by mutual agreement on a date agreed upon by the Bank and the Account Holder,
- (iv) upon the death or termination of the Account Holder without legal successor,
- (v) upon termination of the Account kept with each bank involved in the Service - irrespective of the reason for termination.

8.2.   Simultaneously with the termination of an account contract of an Account of the Account Holder included in a particular Service of the Account Holder, the Contract authorising the use of the services of the Electronic Banking System shall automatically terminate with respect to the terminated Account Contract.

8.3.   The Account Holder may terminate the Contract with immediate effect at any time (whether by ordinary notice or extraordinary notice), whereas the Bank may terminate the Contract upon two (2) months' notice without the obligation to give reasons in a written statement sent to the other Party (ordinary notice), provided that, if the notice of termination of the Account Holder indicates a longer period, the Contract shall be terminated upon the expiry of such longer period.

8.4.   The Bank is entitled to terminate the Contract with immediate effect and terminate the User's access to the Electronic Banking System (deactivation of a given Service) if the Account Holder and/or its Users fail(s) to comply with the terms and conditions of the Contract and the GTC (including in particular the provisions on the safe use of the Electronic Banking System) and seriously or repeatedly breach their obligations set out in the GTC (extraordinary termination).

8.5.   In the event of immediate termination initiated by the Bank, the Bank shall terminate the Account Holder's and all its Users' right to use the given Service at the time when the notice is sent, whereas in the case of ordinary termination, upon the expiry of the notice period.

8.6.   Upon termination of the Contract for any reason, the Bank and the Account Holder/Customer shall make a settlement with each other in accordance with the provisions of these GTC and the General Terms of Contract on the

.

management of the Accounts of the Account Holder kept with the Bank/Investment Business Rules, therefore any cost and fee not paid to the Bank shall become due in full on the date of termination of the Contract.

8.7.   Termination of the Contract for any reason shall not affect the Account Holder's other contractual relationship with the Bank.

9. FEES AND CHARGES

9.1.   The Account Holder shall pay transaction fees, costs, commissions (collectively "**Bank Charges**") for the use of the Electronic Banking System, for orders submitted through the Erste Electra Program in such a way that the Bank debits any due Bank Charge from the Account Holder's Bank Account at the due date specified in the Announcement. The Bank's Announcement in effect from time to time contains the fees, charges and interest rates applicable to the Bank Account, the method of their payment and their due date.

9.2.   The Account Holder shall bear the cost of using the telephone line, internet access and other related costs associated with the use and operation of the Erste Electra System on the user's side.

10. PROVISION OF INFORMATION TO CUSTOMERS

10.1.   General Information
At the request of the Account Holder, the Bank shall, at any time during the existence of the legal relationship with respect to the Service, make these GTC, the applicable Business Rules and the applicable Announcement, Fee Schedule available on paper or on a durable medium, furthermore the effective version of these documents are also available and accessible to the Account Holder at all times in Branch Offices or Company Office and on the website of the Bank.

10.2.   Information provided before a payment order is submitted in connection with the services under the Contract
Before submitting a payment order, the Account Holder receives prior information on the duration of the execution of the payment order, the amount and due date of any fees, costs or other payment obligations payable to the Bank subject to Section 22 (2) of the Payment Services Act in the relevant Announcement in respect of a Bank Account, which are published in the Branch Offices, Company Offices and on the website of the Bank.

10.3.   Subsequent information on payment orders sent through the Erste Electra System (account statement)
The Bank shall inform the Account Holder on payment orders made through the Erste Electra Program, such as debits, crediting, references/data enabling to identify payment transactions in the Bank Account/Investment Account; the amounts of payment transactions calculated in the currency specified in the payment orders, any fees, charges or other payment obligations payable to the Bank, the exchange rates applied by the Bank, the amount prior to the conversion, the value date of the debit in an account statement in accordance with the Account Contract relating to the Contract. The Bank shall prepare the account statement and make it available to the Account Holder in the manner and with the frequency specified in the Account Contract and/or in an additional agreement made to that effect.

11. COMPLAINTS, COMPLAINT MANAGEMENT, RECTIFICATION

11.1. The Account Holder may exercise its right to lodge a complaint about the use of the Electronic Banking System and each bank transaction in accordance with the provisions of the Business Rules.

11.2. The Bank and the Account Holder agree that the Account Holder may request that the the Bank shall rectify an unauthorised or authorised, but not appropriately executed payment order immediately after the Bank receives the payment order sent through the Erste Electra Program, but no later than 30 days after the closing date of the account statement containing the given payment order. The Account Holder may forward its request for rectification in writing to the Bank's account servicing Company Office, enclosing documents or certificates necessary for ruling on the request. If the Account Holder fails to make such documents and data available for the Bank even after a notice by the Bank requesting so, within 15 days upon the receipt of the Bank's notice by the Account Holder, the Bank may dismiss the request without any consideration on the merits, and without any measure taken. If the Bank accepts the request for rectification, the Bank shall credit the amount to be reimbursed in relation to the request to the Account Holder's Account.

.

12.   RULES ON THE MODIFICATION OF THE GTC, THE RELEVANT ANNOUNCEMENT

12.1. If an issue related to a given Service is not regulated by these GTC, the Bank's Financial Business Rules and Announcement, the GTCs concerning payment services available through the Erste Electra System or the Announcement and the applicable provisions of law in effect from time to time shall govern.

12.2.   The Bank shall be entitled to unilaterally modify any interest rate or charge (e.g. fees, expenses and commissions etc) or other contractual conditions of a given Service determined in the relevant Announcement or in the Contract. The Bank may unilaterally modify the Contract in a way that is unfavourable for Account Holder and its Users if any or all of the following conditions and circumstances arise(s):

(i)   a change in the legal or regulatory environment; which may, *inter alia*, be
  − any change in law, decrees of the central bank or official requirements relating to or affecting the activities and operating conditions of the Bank,
  − negative change in the sovereign credit rating regularly   published by international credit rating agencies (recognised external credit rating agency),
  − an increase in payment obligations of the Bank relating to public liabilities (e.g. duties, taxes),
  − adverse changes to the rules on mandatory reserves.

(ii)   changes in the conditions existing in the domestic or international money or capital markets, in the macro-economic environment; which may, inter alia, be:
  − changes in the costs of funding for the Bank,
  − changes in the base rate of the central bank, interest rates quoted by the central bank for repurchase agreements (refinancing) or deposit interest rates,
  − changes in opportunities for fund raising in money or equity markets,
  − changes in money market or equity market interest rates, refinancing and reference interest rates,
  − changes in the interbank borrowing rates,
  − changes in the consumer price indices,
  − an increase in the yield of securities publicly issued by the Bank,
  − an increase in the yield of government securities with a maturity exceeding a year.

(iii)   changes in the risks associated with provision of a given Service and the Account Holder, including
  − an increase or decrease in the annual net sales of the Account Holder.

(iv)   any change in the provision of a given Service and in the operating conditions of the Bank, including:
  − adverse changes in bank costs paid for the use or lease of technical devices, property used by the Bank,
  − adverse changes in bank costs paid for ensuring physical, information technology and security technology conditions,
  − adverse changes in bank costs arising from changes in the requirements of IT and data protection applications,
  − changes in external and internal processes, procedures relating to banking services, the use of banking services, as well as IT and security technology related conditions,
  − adverse changes in the operating costs of the Bank,
  − adverse changes in the conditions and fees or charges of postal, telecommunications, internet service,
  − adverse changes in fees, commissions, costs charged or passed on by third party service providers for the provision of services,
  − adverse changes in fees, commissions, costs relating to interbank settlements.

At a given point of time, the afore-mentioned conditions may change contrary to one another or differently in their proportion /increase, decrease/. At all times, the Bank takes into account the conditions that have an actual effect at a given point of time, in proportion to their effect, when determining the concrete extent of conditions.

12.3.   The Bank shall initiate any unilateral modification to the Contract – including these GTC and the relevant Announcement – that has an adverse effect on the Account Holder or the User, on paper or on a durable medium at least 2 months before the date which the Bank determines for entry into force. The Bank deems such modifications accepted by the Account Holder if the Account Holder accepts the modification until the day that precedes the effective date of modification specified by the Bank or the Account Holder fails to notify the Bank on its non-acceptance of the modification until the day that precedes the effective date of modification. If the Account Holder does not accept the modification and notifies the Bank accordingly in writing until the day preceding the effective date of the modification, the Bank deems the non-acceptance of such modification as termination with immediate effect by the Account Holder. In the event of such termination, the Bank does not charge any fee or cost for termination, but any and all payment

obligations of the Account Holder outstanding vis-a-vis the Bank shall become due and payable upon such termination and shall be paid and discharged upon termination.

12.4.   If the modification of the Contract is intended to terminate any service provided by the Bank, the Bank and the Account Holder or the User/Securities User shall settle their accounts, including in particular the fees paid in advance by the Account Holder or the User/Securities User. In this case, the Bank shall be entitled to a pro-rated consideration for the service actually provided. If the Account Holder is deemed to be a microenterprise under Section 2 (17) of the Payment Services Act, the Bank shall not charge any fee, expense or other payment obligati on for settlement.

12.5.   The Bank shall be entitled to initiate any modification of the conditions of the Contract – including the present GTC and the relevant Announcement – fees, costs and interests where such modification has no adverse effect on the Account Holder and the User at any time, unconditionally, and the Account Holder expressly approves this stipulation upon the execution of this Contract. The Bank shall inform the Account Holder about such modification and the effective date, by hanging the modified documents - the GTC, the applicable Announcement - in the Bank's Branch Offices and the Company Offices on the banking day preceding the effective date of the modification and publish the amended GTC and/or relevant Announcement and/or Business Rules o n its website.

13. OTHER PROVISIONS

13.1. The Bank shall become exempt from liability if it proves that the [non -]fulfilment of its obligation defined in these GTC was caused by a circumstance beyond its control, unforeseeable at the date of conclusion of the Contract, and the Bank acting with due care could not avoid such circumstance or damage, or the fulfilment of such obligation was frustrated by the provisions of law or Community legal acts.
When there is a change in law affecting the provisions of these GTC that credit institutions are obliged to comply with by the mandatory operation of the law, the new or amended provision of law shall be deemed as incorporated in these GTC.

13.2.   The detailed rules for the processing of the personal data of private individuals using the Services, which are processed by the Bank in connection with the use of the Services, are set forth in the Bank's Business Rules (available at: https://gate.erstebank.hu/uzletszabalyzat),   and   the   Data   Protection   Notice   (available   at: https://www.erstebank.hu/hu/adatkezelesi).

13.3.   Where any document refers to a specific clause of any of the General Terms and Conditions indicated below, it shall be construed in accordance with the corresponding provision in the Customer Notice or in these GTC.

13.4.   These amended and restated GTC enter into force on **1 December 2022** and simultaneously the GTC under the title Commerzbank Electronic Banking General Terms and Conditions in effect from 30 September 2019 shall cease to be effective.

Commerzbank Zrt.   **Erste Bank Hungary Zrt.**

COMMERZBANK ◣

General Terms and Conditions of the Electronic Banking service

Annex 1: Technical specifications

1. Minimum hardware and software requirements for the use of Archive Electra Software:

1.1   Minimum hardware environment for running the Program:

- IBM PC compatible computer
- 60 Mb of free disk space (the program only takes up about 25 MB when installed, the rest is reserved for later operation)
- Minimum 1024x768 resolution display (at least in 256 colour mode)
- Min. 32 MB memory (can run on 16 Mb, but cannot handle larger files)
- CD drive
- printer

1.2   Minimum software environment for running the Program:

- Windows 7 or newer operation system
- Microsoft Internet Explorer 6.0 or Mozilla Firefox 3.0III

2. Minimum hardware and software requirements for using the Global Payment Plus application:

discontinued from 01 December 2022

3. Minimum hardware and software requirements of Erste Electra Program are available on the website of Erste Bank Hungary Zrt.:

3.1 Minimum hardware environment for running the Erste Electra Program:

- Computer (or other smart device) with Intel Pentium 4 or equivalent processor, with 512 MB RAM
- Internet connection

3.2 Minimum software environment for running the Erste Electra Program:

- Windows 7, Windows 8, Windows 8.1., Windows 10 or newer operation system
- Microsoft Internet Explorer 6.0 or Mozilla Firefox 3.0III

The current version of the requirements are available at

www.erstebank.hu

```
https://www.erstebank.hu/hu/ebh-business/kisvallalkozasok-mikro/mindennapi-
bankolas/elektronikus-bankolas/erste-
electra#/modalComponent/isOpen/true/url/%2Fhu%2Ftudastar%2Fvallalatok%2Fminde
nnapi-bankolas%2Felektronikus-szolgaltatasok%2Ferste-electra%2Fmilyen-
technikai-feltetelek-szuksegesek-az-erste-electra-hasznalatahoz.question
```

.