# BUSINESS TERMS AND CONDITIONS FOR THE PROVISION OF ELECTRONIC BANKING SERVICES

## UniCredit Bank Czech Republic and Slovakia, a.s., pobočka zahraničnej banky

UniCredit Bank

1. UniCredit Bank Czech Republic and Slovakia, a.s., Želetavská 1525/1, 140 92 Prague 4 - Michle, ID No.: 649 48 242, registered in the Companies Register of the Municipal Court in Prague, Section: B, File No.: 3608, conducting banking activities in the Slovak Republic through UniCredit Bank Czech Republic and Slovakia, a.s., pobočka zahraničnej banky, Šancová 1/A, 813 33 Bratislava, ID No.: 47 251 336, registered in the Companies Register of the Bratislava III Municipal Court, Section: Po, File No.: 2310/B (hereinafter referred to as the "Bank"), provides its clients for whom it maintains accounts (hereinafter referred to as the "Account Owner/Account Owners" or the "Client/Clients") with the electronic banking service based on a contract allowing the Clients, when using the relevant device, to handle the agreed banking products (such as account, loan, payment card, bank guarantee, insurance, investment instrument, etc.), to enter into the relevant product contract (hereinafter referred to as the "Product Contract") as well as secure communication between the Client and the Bank via the Internet (hereinafter jointly referred to as the "EB Services").

2. EB Services may be provided via the Online Banking, BusinessNet Professional, BusinessNet and UC Trade Finance Gate web apps (hereinafter referred to as the "EB Web Apps"), via the Smart Banking, Business Smart Banking and BusinessNet Mobile mobile apps (hereinafter referred to as the "EB Mobile Apps", together with the EB Web Apps hereinafter jointly referred to as the "EB Apps") or via an offline service (Multicash). The term "device" means, in particular, a mobile phone, tablet, computer or any other device from which it is possible to log in to electronic banking and use the EB Services.

3. These Business Terms and Conditions for the Provision of Electronic Banking Services of the UniCredit Bank Czech Republic and Slovakia, pobočka zahraničnej banky (hereinafter referred to as the "Business Terms and Conditions") shall define a part of the contract between the Bank and the Client, the subject-matter of which is the agreement on provision of the defined EB Service (hereinafter referred to as the "Contract" ) and they shall define the binding rules for relationships between the Bank and the Client in relation to the provision of EB Services. These Terms and Conditions enter into force on 1 June 2026 and shall fully replace the Terms and Conditions for the Provision of Electronic Banking Services effective as of 1 April 2025.

## 1. GENERAL PROVISIONS

**1.1** The Bank shall provide EB Services under the terms and conditions stipulated in the relevant Contract and, further, in compliance with the applicable legal regulations, General Business Terms and Conditions of the Bank for the Performance of Banking Deals (GBTC), these Business Terms and Conditions, Business Terms and Conditions of the Bank for the Provision of Payment Services and, as the case may be, in compliance with other contractual documents depending on the type of the agreed EB Service. If the use of the relevant EB Service is subject to a fee, the fee is specified in the Price List of Banking Services applicable to the relevant segment (hereinafter referred to as the "Price List"). In such a case, the Bank is entitled to charge the relevant fee specified in the Price List and the Client is obliged to pay it.

**1.2** An overview of the available services and functionalities, as well as a list of technical requirements for the devices used to access the EB Services, is provided in the respective overview of Electronic Banking Services and Parameters (hereinafter referred to as the "Overview of Services"). The currently valid Overview of Services is published on the Bank's website wwww.unicreditbank.sk and is also available at the Bank's points of sale.

**1.3** If technically feasible, the agreed EB Services may be used as a means of distance communication between the Client and the Bank or the Client and a third party, including for the submission of proposals for the conclusion of a Product Contract and for the notification of acceptance of a draft Product Contract, including any amendments thereto. When concluding contracts at a distance via the relevant EB Service, authorisation using the personalised security feature shall be equivalent to the Client's signature on a paper medium.

**1.4** The Bank shall inform the Client via EB Services about the fund balances on accounts and about the transactions made. The Client is obliged, either in person or through the User (clause 2.1 below) to check, from time to time, whether the settlement reports correspond to the orders made and whether the orders made were implemented or rejected by the Bank. The Client is obliged to inform the Bank about discovered errors in settlement or other discrepancies without undue delay.

**1.5** Information and documents sent by the Bank to the Client via EB Services shall be considered delivered on the date on which they are delivered to the mailbox of the relevant EB App and reach the Client.

**1.6** Based on technical and business developments, the Bank may add new apps and functions within EB Services and remove outdated apps and functions, change apps, their names and their functionalities. In order to ensure the highest possible level of security of the EB Services, the Bank is also entitled to terminate the use of personalised security features or to modify their settings in the event that, due to causes beyond the Bank's control, there is a risk of a reduction in their level of security, upon prior notification to the Client via the EB App to which the modification relates or, the event of a consumer, in writing no later than 2 months prior to the date on which the change in the app settings is to take place.

**1.7** The Bank is entitled to available to the Client all the currently offered IB Services and may connect all its currently opened and future accounts, payment cards and other products of the Bank to them. The Bank shall allow the Client, at the Client's request, to change the set of accounts connected to individual EB Services, the level of authorisation and the amount of limits.

## 2. ELECTRONIC BANKING SERVICE USERS

**2.1** The EB Service User is the person who has access to EB Apps as:

**a)** the Account Owner or co-applicant for a banking deal, if they use EB Services;

**b)** the user permission administrator (hereinafter referred to as the "Administrator") as defined below;

**c)** another person to whom the Account Owner or the Administrator has granted authorisation to use the EB Services

(any of these persons hereinafter referred to as the "User").

**2.2** The Account Owner is liable for ensuring that the Bank always has up-to-date personal data of the User in order to properly identify the User.

**2.3** An Administrator is a special category of User who has been authorised by the Account Owner to grant, change or remove user profiles in EB Apps to other Users including the Account Owner.

**2.4** The User's access to EB is conditional upon the conclusion of the Contract with the Account Owner and the User's acceptance of the Business Terms and Conditions.

**2.5** By authorising the User, the Account Owner grants their consent to the Bank to provide or make available to the User and, as the case may be, to the telephone numbers or e-mail addresses specified by the Account Owner, any information notified by the Bank to the Account Owner in relation to use of EB Services, which would otherwise be subject to banking secrecy or protection according to the personal data protection regulations.

**2.6** The User's authorisation expires:

**a)** on the date of cancellation of the last banking product to which User's authorisation granted in the EB App relates;

**b)** upon written withdrawal of the authorisation by the Account Owner or the Administrator;

**c)** upon termination of the authorisation by the User;

**d)** upon death of the User.

**2.7** The User's access to EB Services shall be terminated no later than the end of the next working day following the date of receipt of the Account Owner's or the Administrator's notice or termination of User's authorisation by the Bank, unless a later date is specified therein.

**2.8** If there is a change in the composition of the statutory body that was a User, its status as a User shall remain until a new User is set up on the basis of the relevant instruction delivered to the Bank by the Account Owner.

## 3. ELECTRONIC BANKING SERVICES SECURITY RULES

**3.1** Terms and characteristics of personalised security features:

| | |
|---|---|
| **PIN for mobile app** | A numeric code for the EB Mobile App that is used to activate, log in or authorise transactions. |
| **Password for login** | The password consists of numeric characters (6 characters). It is used for logging in to EB Web Apps in combination with a one-time SMS code. The User is obliged to immediately change the initial password provided to the User by the Bank. |
| **Security Key (Smart Key, Business Key)** | The function contained in the EB Mobile Apps is intended for logging in to the EB Apps or for authorising payment transactions and other requests or for generating one-time codes for logging in or authorising transactions in the EB Web Apps even without connecting the device to the Internet, i.e., in the offline mode. |
| **Hardware security key (token)** | A PIN-protected hardware device designed to generate one-time numeric codes for logging in or authorising transactions in EB Web Apps. |
| **SMS Key** | A combination of a password and one-time codes sent via SMS to the User's mobile phone to log in or authorise transactions in EB Web Apps. |
| **Registered mobile telephone number** | A telephone number notified by the User to the Bank that allows the receipt of one-time security codes, called SMS OTP. |
| **Registered e-mail address** | An e-mail address notified by the User to the Bank that allows the receipt of one-time security codes (OTP e-mail). |
| **Fingerprint (biometrics)** | A fingerprint stored on the mobile device on which the EB mobile app is activated. |
| **Face scan (Face ID) (biometrics)** | A face scan stored on the mobile device on which the EB mobile app is activated. The face scan is compared with biometric data stored with the Bank or against a photograph (e.g., from an identification document). |
| **Password** | A password consisting of various alphanumeric characters used to authenticate the User in various situations. |
| **One-time security password** (OTP = One-Time Password) | A one-time security code that can be used to verify ownership of the security feature. It is a code sent to a registered mobile telephone number, registered e-mail address or generated by the EB mobile app. |
| **Username** | An assigned or, in some cases, separately configurable username (alias) for logging in to the EB App. |
| **User number** | A number assigned to the User by the Bank. |
| **Identity document** | A User's document issued by a public authority, stating the name and surname, the date of birth and showing the appearance (e.g., ID card, driving licence, passport). |

| | |
|---|---|
| **Birth certificate number** | The User's birth certificate number. |
| **Control question** | A questions about the User or the User's products. |
| **CVV2/CVC2 code** | A special three-digit number that appears on the payment card. It is a security feature used to identify the card holder in an environment without the presence of a payment card (e.g., the internet). |
| **Payment card number** | Unique 16-digit payment card number. |
| **Electronic signature** | Designation of specific data that replaces the User's handwritten or verified signature in the computer. |

**3.2** The User is obliged to familiarise themselves with the following:

**a)** the setup options for personalised security features;

**b)** the setup options for personalised security limits to limit the amount of the payment transaction;

**c)** the following obligations regarding the protection of personalised security features and the procedure in the event of loss, theft, misuse or unauthorised use of a personalised security feature.

**3.3** The User is obliged to take appropriate measures to protect its personalised security features so that they cannot be lost, misused or used in an unauthorised manner. The User is obliged in particular:

**a)** not to use passwords and PINs in other apps and on the internet (e.g., e-shops, social networks, e-mails, etc.) that are identical to the passwords and PINs used to log in to the EB or to authorise payment transactions;

**b)** to set the password or PIN so that it is not easily guessed or inferred, e.g., by combining lower and upper case letters, numbers, special characters, etc;

**c)** not to disclose to others or enter their personalised security feature anywhere on the internet except when logging into the EB Web Apps at https://sk.unicreditbanking.eu, https://sk.unicreditbanking.net/ or https://corporateportal.unicreditgroup.eu/container/sk/login;

**d)** do not write down passwords and PINs, protect them from disclosure and change them immediately if they have been disclosed or if the User merely suspects that such a situation has occurred;

**e)** to take extra care when entering personalised security features in public (e.g., on public transport vehicles) or in monitored rooms (e.g., near security cameras) so that they cannot be seen by others;

**f)** not to log in to electronic banking unless the User is sure that no malicious software can be installed on the device or if the device is not completely under the User's control (e.g., in public internet cafes, on computers used by several people);

**g)** to give the password for communication with the Bank only to a Bank employee in a situation where this password is required;

**h)** to protect SIM unlocking and use in a mobile device with a PIN and have the SIM card blocked immediately by the operator if the mobile device is lost or stolen;

**i)** to protect the User's profile with the mobile operator and not to allow a third party to issue a new SIM/eSIM for the User's phone number;

**j)** not to allow others to access their e-mail account and set up two-factor authentication;

**k)** not to allow another person access to their mobile device (e.g., fingerprint, face scan, password, PIN);

**l)** if the mobile phone or SIM card is lost or stolen, to notify the Bank immediately and have the EB Services blocked as a precaution;

**m)** not to allow the registration of biometric data of another person (or family member) on a mobile device;

**n)** to secure access to the mobile device with a password, PIN or biometric (fingerprint, face scan) and not to leave their mobile device unattended or automatically lock the device screen after a short period of time;

**o)** not to use software modifications to the mobile device that allow full administrator access (e.g., jailbreak, root);

**p)** to regularly update the operating system of the mobile device and individual installed apps;

**q)** to use the latest version of security software (e.g., antivirus, firewall) on the mobile device;

**r)** not to allow unnecessary permissions in newly installed or updated apps on the mobile device (e.g., access to SMS, settings facilitation, etc.);

**s)** to install only apps from the official app stores – Google Play (Android), App Store (iOS) – including any add-ons. If the app used requires them to install it in their mobile phone, set the mobile device to prohibit the installation of apps from unknown sources;

**t)** not to install apps based on third-party instructions or request and not to allow a third party access the mobile phone remotely (e.g., via the AnyDesk app);

**u)** not to log on to a computer as an administrator unless necessary, but as a regular user;

**v)** to regularly update the operating system and their programs, especially the web browser. To install browser extensions (plug-ins) on a limited basis and only from known and trusted publishers;

**w)** to use the latest version of security software (e.g., antivirus, firewall) and update it regularly;

**x)** to protect the computer from unauthorised access of other persons by setting access permissions, password security or other features. Not to allow a third party remote access to the computer (e.g., via AnyDesk apps);

**y)** to enter the Bank's website address manually. To access the EB Web App, use the Bank's website www.unicreditbank.sk, from there go to the internet banking login page, check that the access is to the websites https://sk.unicreditbanking.eu, https://sk.unicreditbanking.net/ or https://corporateportal.unicreditgroup.eu/container/sk/login and not to use a shortcut to the internet banking login page;

**z)** not to access EB Services via a link from a search engine or a link sent by e-mail, SMS or other means (social network, chat app, etc.);

**aa)** not to log in if the login screen for EB Services looks suspicious to the User;

**bb)** to contact the Bank without delay if the User registers a transaction that the User did not authorise;

**cc)** not to respond to telephone calls that encourage the User to take action with the account, as the Bank never encourages its Clients to make any transactions by telephone;

**dd)** not to open an e-mail containing the Bank's name unless it comes from the domain: unicreditbank.sk or unicreditgroup.sk, not to open attachments of non-standard file type (e.g., file extensions: .exe, .php.) and not to click on links contained in the suspicious message;

**ee)** to familiarise themselves with the messages sent by the Bank to EB Services, in particular regarding fraud warnings.

**3.4** If the User:

**a)** is a minor, the legal guardian is responsible for protecting the personalised security features and the safe use of the EB Services;

**b)** is represented by a court-appointed guardian, the guardian is responsible for protecting the personalised security features and the safe use of the EB Services.

## 4. LOGGING IN TO THE APP, AUTHENTICATING THE USER, ACTIVATING THE APP. AUTHORISING A PAYMENT TRANSACTION, NON-PAYMENT ORDER OR SETUP INSTRUCTION

**4.1** When logging in to the EB App, the Bank authenticates the User through the relevant combination of personalised security features of the User.

**4.2** The User authorises a payment transaction, activates the relevant EB App, provides consent to enter into the Contract, grants the Bank a non-payment order, instructs the Bank to set up EB Service, etc. by properly using its personalised security features and pressing the confirmation button.

**4.3** The Bank shall execute a payment transaction or setup instruction if it contains complete data conforming to the prescribed forms and is authorised in accordance with the relevant EB App in accordance with the Contract and the Business Terms and Conditions. The Bank shall not be liable for any damage resulting from the non-execution of payment orders that do not meet the conditions for their execution.

**4.4** In the EB Mobile Apps, activation is performed using an activation code generated by the Bank and delivered to the User via SMS, and entering a PIN.

**4.5** In the EB Mobile Apps, authorisation takes place in one of the following ways, after the User is prompted to do so:

**a)** by fingerprinting or by attaching (scanning) the User's face to the device;

**b)** by entering a PIN code.

**4.6** In the EB Web Apps, login and authorisation is performed in one of the following ways:

**a) With a security key, namely:**

**(i)** Smart Key – an online method – the User receives a push notification in the EB Mobile App and then confirms the transaction using fingerprint, facial scan or by entering a PIN;

**(ii)** Smart Key – an offline method – the EB Web App displays a QR code, which the User scans via the Smart Key in the Smart Banking Mobile App, which generates a 6-digit one-time code. The User enters this code into the Online Banking Web App login section and confirms it;

**(iii)** Business Key – an offline method for logging in to the BusinessNet Professional, BusinessNet and UC Trade Finance Gate apps – the User generates a 6-digit code for logging in via the Smart Key in the Business Smart Banking or BusinessNet Mobile mobile app.

**b) SMS Key**
This method consists of a combination of a personal password and one-time codes sent to the User's mobile phone. The User enters their password on the EB Web App screen and the Bank sends an SMS message to the User's designated mobile phone in the form of an SMS containing the one-time code. The User enters this time-limited code back into the EB Web App to confirm the transaction.

**c) Hardware security key (token)**
The password for signing a transaction is generated by a token. The User enters the PIN directly on the token keypad. If the correct PIN is entered, the token generates an 8-digit one-time code that the User enters in the Web App. The App then displays a 6-digit one-time code, which the User enters again in the App to authorise the transaction.

**4.7** In the Multicash service, authorisation is carried out via an electronic signature based on a password entered on the client side. The electronic signature is used to sign and encrypt the data file, which can then be sent to the Bank for processing.

**4.8** A payment transaction is cancelled in the same way as its authorisation, if the cancellation is enabled by the respective EB App.

**4.9** In EB, the User can use the payment services of indirect payment order entry and the payment account information service.

**4.10** The Bank is entitled to change the method of User's authentication, authorisation of payment transactions and other legal actions primarily for the purpose of enhanced security of the EB Services. The Bank shall inform the User of the new authentication or authorisation method via the EB App to which the change relates or in writing at least two months before the date on which the change is to take effect.

## 5. LIABILITY FOR UNAUTHORISED PAYMENT TRANSACTIONS

**5.1** The User is obliged to notify the Bank without undue delay, but no later than 13 months from the date on which the amount of the payment transaction was debited from the account, of an unauthorised transaction, loss, theft, misuse or unauthorised use of a payment instrument or personalised security feature, personal documents, mobile phone with a stored payment card, with mobile banking activated or anything suspicious in connection with electronic banking.

The place for reporting is the Bank's Customer Service Line (Infoline), which is listed on the Bank's website in the "Contacts" section and is available 24/7 (non-stop), or at any of the Bank's branches during their operating hours. The Bank provides information on the manner in which the User is required to notify the loss, theft, misuse, or unauthorized use of personal security features, payment instrument, or Electronic Banking Services (EB Services) on its website and at its branches.

**5.2** The Account Owner shall bear a loss of up to EUR 50 which is related to all unauthorised payment transactions and which is caused by using a lost or stolen payment instrument or misusing a payment instrument by an unauthorised person as a result of the User's negligence in securing personalised security features, except as provided below.

**5.3** The Account Owner shall not bear financial loss if:

**a)** it results from the use of a lost, stolen or misused payment instrument from the moment of reporting this fact to the Bank; this does not apply if the User has acted fraudulently;

**b)** the loss, theft or misuse of the payment instrument could not have been detected by the User prior to the payment transaction; this does not apply if the User has acted fraudulently.

**5.4** The Account Owner shall bear all losses related to unauthorised payment transactions if they are caused by the User's fraudulent conduct, the User's wilful failure to comply with one or more of the User's obligations to provide personalised security features, or the User's gross negligence in failing to comply with one or more of these obligations.

## 6. SPECIAL LIABILITY PROVISIONS

**6.1** The User is not entitled to make copies of the contents of the program media and is obliged to use only devices that cannot, due to defects including infection, endanger or prevent the operation of the Bank's systems.

**6.2** The Account Owner shall be liable for any damage incurred by the Bank or third parties as a result of, for example, the transmission of a computer virus from the device used in relation to EB Services.

**6.3** The Bank shall not be liable for the compatibility of the EB App with other app equipment on the User's device. The Bank shall not be liable for damage and malfunctions or loss of functionality of the mobile phone and the mobile phone app equipment resulting from the mobile phone being damaged or having other defects not meeting the characteristics stated by the manufacturer or containing app equipment incompatible with the EB App.

**6.4** If the User is provided with access to product information provided by third parties through EB Services, the Bank shall not be liable for the accuracy or availability of such information.

**6.5** The Bank shall not be liable for any damage resulting from the following:

**a)** technical failure of the client's device, malfunctions of the telephone network or the public data network, breach of secrecy of the transmitted messages that the Bank could not influence, application of international sanctions within the meaning of the legislation on the implementation of international sanctions, or other circumstances that exclude the Bank's liability;

**b)** unauthorised use of certification and authorisation tools and other personalised security features in the period between their invalidation by the User and the automatic transfer of this information from the registration (or certification) authority to the Bank's system.

## 7. ELECTRONIC BANKING SERVICES AVAILABILITY AND BLOCKING

**7.1** The User may use EB Services 365 days a year and 24 hours a day, unless the Bank does not allow access to the EB Services for the following reasons:

**a)** when necessary for the maintenance of banking systems, apps or data processing;

**b)** if the User logs in to the EB Apps from an IP address that is located in a geographical area subject to international sanctions or other security rules of the Bank. The Bank lists these geographical areas on its Website;

**c)** if the User logs in to the EB Apps from an IP address that shows suspicious activity (e.g., bulk sending of unsolicited commercial messages, chain messages, participation in hacking attacks);

**d)** if it is caused directly or indirectly by circumstances beyond the control of the Bank as a result of force majeure, natural disasters, hardware malfunctions, computer viruses or other events caused, for example, by a third party.

**7.2** The Bank is entitled to block EB Services or the User's access to them:

**a)** if the User violates, in a serious manner or repeatedly, the User's obligations arising for the User from the contractual relationship with the Bank;

**b)** if the Bank has a reasonable suspicion that unauthorised or fraudulent use of the EB Service has occurred or if there is a reasonable suspicion that such use may occur;

**c)** if the Bank's legitimate interest is at stake;

**d)** in case of an increased risk that the Account Owner will not be able to repay the loan granted by the Bank.

**7.3** The Bank shall inform the specific User and Account Owner about blocking the EB Service on the Bank's initiative before the blocking is executed or immediately after the blocking is executed in an appropriate manner, unless informing the relevant person would defeat the purpose of the blocking or would be contrary to the law.

**7.4** If the EB Service is blocked, the indirect payment order service cannot be used.

**7.5** The costs associated with User-initiated blocking shall be borne by the Account Owner, unless the Bank is obliged to carry out such blocking after the User notifies the Bank of the misuse or theft of a payment instrument or personalised security feature.

## 8. SPECIAL PROVISIONS FOR OFFLINE EB SERVICES

**8.1** Prior to making the offline EB Services available, the Bank shall, upon request of the Account Owner, provide the User with professional training on the use of such services, unless they have been provided to the User by a third party, i.e., not by the Bank or its authorised person. In case the respective offline EB Service has been provided to the User by another licence rights owner, the Account Owner confirms by signing the Contract that the Account Owner has been fully familiarised with the relevant service and does not require training by the Bank or its authorised person to use such EB Service.

**8.2** The Bank provides offline EB Services as ordered.

**8.3** The User is obliged to test the EB Service system and establish an initialisation connection with the Bank when starting to use the relevant offline EB Service.

**8.4** The initial date of use of the offline EB Service is the date on which:

**a)** the User has received from the Bank the installation medium for the relevant EB Service and/or the certification and authentication tools in the case where the Bank provides the relevant EB Service to the Account Owner;

**b)** the User has received the certification and authentication tools from the Bank in case the User has been granted access to the offline EB Service by another licence rights owner;

**c)** the installation media for the system for the provision of the offline EB Services and/or the certification and authentication tools as ordered;

**d)** the Bank has made the relevant settings.

**8.5** Before transferring individual data files, the User is obliged to save the transferred data in full so that the Bank or a person authorised by the Bank can check them at any time. The User is obliged to keep these records for at least thirty working days from the date of their dispatch to the Bank. During this period, the Bank is entitled to inspect these records and the User is obliged to allow the Bank or a person authorised by the Bank to do so.

**8.6** The User agrees to maintain the confidentiality of all messages received from the Bank, even after the end of the use of the EB Services.

## 9. FINAL PROVISIONS

**9.1** The Parties shall be entitled to terminate the Contract in writing at any time. If the Contract is terminated by the Client, it shall expire on the first working day following the date of delivery of the notice to the Bank or on a later date specified in the notice; if the Contract is terminated by the Bank, it shall expire two months after the date of delivery of the notice to the Client, unless it is a notice on grounds of fraudulent conduct of the User, which shall enter into effect on the date of delivery thereof to the Client.