PRODUCT BUSINESS TERMS AND CONDITIONS FOR INTERNET AND ELECTRONIC BANKING

UniCredit Bank Czech Republic and Slovakia, a.s.

UniCredit Bank

Content

UniCredit Bank

PREAMBLE

1. UniCredit Bank Czech Republic and Slovakia, a.s., ID No. 64948242, registered in the Companies Register of the Municipal Court in Prague, Section B, File No. 3608, (hereinafter referred to as the "Bank"), provides its clients for whom it maintains accounts (hereinafter referred to as the "Clients" or the "Account Owners") with the service of internet and electronic banking (hereinafter referred to as the "IEB") based on the respective contract allowing the Account Owners, when using the relevant device, to handle the agreed banking products, such as account, payment card, loan, bank guarantee, insurance, investment, 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 "Internet and Electronic Banking Products" or the "IEB Products"). IEB Products are available both in internet banking (hereinafter referred to as the "IB") and electronic banking (hereinafter referred to as the "EB").

IB may be provided via the Online Banking, BusinessNet Professional, BusinessNet and Trade Finance Gate web apps (hereinafter referred to as the "IB Web Apps") and via the Smart Banking, Business Smart Banking and BusinessNet Mobile mobile apps (hereinafter referred to as the "IB Mobile Apps"), (hereinafter jointly referred to as the "IB Apps"). EB may be provided via Eltrans 2000 (Gemini 5.0) and MultiCash apps (hereinafter referred to as the "EB Apps"). "IB Apps" and "EB Apps" shall hereinafter jointly be referred to as the "IEB Apps". The term "device" means, in particular, a mobile phone, tablet, computer or any other device from which it is possible to log in to internet and electronic banking and then use the IEB Products.

2. These Product Business Terms and Conditions for Internet and Electronic Banking UniCredit Bank Czech Republic and Slovakia, a.s. (hereinafter referred to as the "IEB Product Terms and Conditions") are effective from 1 April 2025, and they shall repeal and supersede the previously effective Product Business Terms and Conditions for the Provision of Internet Banking Products of UniCredit Bank Czech Republic and Slovakia, a.s., the previously effective Product Business Terms and Conditions for the Provision of Direct Banking Products of UniCredit Bank Czech Republic and Slovakia, a.s., and the previously effective Product Business Terms and Conditions for the Provision of Electronic Banking Products of UniCredit Bank Czech Republic and Slovakia, a.s., in their entirety.

1 GENERAL PROVISIONS

1.1 The Bank provides the IEB Products under the terms and conditions laid down by the relevant Product Contract, the General Business Terms and Conditions of UniCredit Bank Czech Republic and Slovakia, a.s., in the version in force at the time of the contractual relationship, unless they are changed pursuant to Article 3 (hereinafter referred to as the "General Business Terms and Conditions"), these IEB Product Terms and Conditions, and the relevant product terms and conditions concerning the Product Contract, and the legislation. If the use of the relevant IEB Product is subject to a fee, the fee is specified in the Price List for the Provision of Banking Services of UniCredit Bank Czech Republic and Slovakia, a.s., applicable to the relevant segment (hereinafter referred to as the "Price List") and 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 of the IEB Products, as well as a list of technical requirements for the device enabling access to the IEB Products, is provided in the respective Overview of Internet Banking Services and Parameters and the Overview of Electronic Banking Services and Parameters while the currently valid overviews of services and parameters are published on the Bank's website www.unicreditbank.cz and are also available at the Bank's points of sale.

1.3 The Bank may amend the IEB Product Terms and Conditions or add new provisions to them if there is a reasonable need for such amendment or addition, for example, the need to amend or newly expressly regulate certain rights and obligations of the Parties following a change in the law, available technology, the situation on the financial markets or the Bank's business policy. The Bank will send the wording of changes and amendments, or the complete wording of such amended IEB Product Terms and Conditions, to the Client at least 2 months prior to the proposed effective date of such amendment by any means agreed for communication between the Bank and Client under the relevant contractual relationship. The Bank may also inform the Client of changes to these IEB Product Terms and Conditions electronically. If the Client does not agree with the proposed amendment to the IEB Product Terms and Conditions, the Client is entitled to terminate the relevant contractual relationship in writing for this reason with effect from the date immediately preceding the effective date of the proposed amendment or, if such right is granted to the Client by law, with immediate effect. If the Client does not reject the Bank's proposal, then the new wording of the IEB Product Terms and Conditions becomes binding upon the concluded contractual relationship as a change in the originally agreed conditions of the contractual relationship, effective as from the date stated in the given amendment to the IEB Product Terms and Conditions as the date upon which the new wording of the IEB Product Terms and Conditions becomes valid.

1.4 Should the parties' rights and obligations governed by the IEB Product Terms and Conditions change as a direct result of a change in legislation that cannot be contractually circumvented, the procedure under the previous paragraph shall not apply. The Bank shall inform the Client of any such change.

1.5 The relevant IEB Apps, if technically possible, may be used as a means of remote communication between the Client and the Bank, or the Client and a third party, and to negotiate remote financial services contracts, including amendments thereto. When negotiating contracts, the authorisation or consent confirmed by the personalised security feature (see Article 3.1) is equivalent to the Client's signature on paper.

1.6 The Bank is entitled to provide the Client with information, send draft contracts and amendments thereto and other relevant correspondence to the IEB. Information and documents sent by the Bank in this way shall be deemed to have been delivered on the date they are delivered to the mailbox of the relevant IEB App or on the date of installation of the IEB services, i.e., the moment they come within the Client's sphere of influence.

1.7 The Bank informs the Account Owners through the IEB Apps about account balances and the transactions executed. The Account Owner is obliged – either personally or through the User as defined in Chapter 2 below – to check whether the orders entered have been executed or rejected by the Bank and whether the settlement reports correspond to the orders entered. The Account Owner is also obliged to check all non-payment transactions, including incoming transactions notified to the Account Owner. The Account Owner or User is obliged to notify the Bank of any defects or other irregularities without undue delay. If the User does not file a claim no later than 30 days of the date of their display in the relevant IEB App, without being prevented from doing so by objective insurmountable obstacles, the claim shall be considered not to have been filed without undue delay.

1.8 Based on technical and business developments, the Bank may add new apps/functions to the IEB and remove outdated apps/functions, change apps, their names and their functionalities. In order to ensure the highest possible level of security of the IEB Products, 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 IEB App to which the modification relates or in writing no later than 2 months prior to the date on which the change in the IEB App settings is to take place.

1.9 The Bank may make available to the Client all the currently offered EIB Products and may connect all its currently opened and future accounts, payment cards and other products of the Bank to these Products. The Bank shall allow the Client to change the set of accounts connected to individual IEB Products, the level of authorisation and the amount of limits.

2 PERSONS USING INTERNET AND ELECTRONIC BANKING

2.1 The person who has access to the IEB Products may be an Account Owner, User Permissions Administrator (hereinafter referred to as the "Administrator") or User depending on the specific role in a given situation. These roles are not mutually exclusive, and therefore a person may act in only one of these roles, in several roles, or in all roles at once.

2.2 The Account Owner is liable for ensuring that the Bank always has up-to-date personal data of the person who has access to the IEB Products in order to properly identify such person.

2.3 The User of the IEB Products is:

a) the Account Owner or co-applicant for the banking service in question, if they use IEB Products, or

b) the Administrator, or

c) another person to whom the Account Owner or the Administrator has granted authorisation to use the IEB Products.

2.4 An Administrator is a special category of User who has been authorised by the Account Owner to grant, change or remove user permissions in IEB Apps to other Users. The Administrator can also grant, change, and remove user permissions for themselves if they have been authorised to do so by the Account Owner.

2.5 The User's access to the IEB Products is conditional upon the User's execution of the applicable contract with the Account Owner and User's acceptance of these IEB Product Terms and Conditions when the User first accesses the IEB Products, unless the User has previously accepted them.

2.6 By designating the User in accordance with the preceding paragraph, the Account Owner consents to the Bank providing that person with any information that would otherwise be subject to bank secrecy and to the Bank accepting on behalf of the Account Owner any documents sent by the Account Owner to the Bank in accordance with Article 1.6. Information and documents sent by the Bank shall also be deemed to have been delivered to the Account Owner on the date on which they are delivered to the User pursuant to Article 1.6.

2.7 The User's authorisation expires:

a) on the date of cancellation of the last banking product to which User's authorisation relates;

b) by the Account Owner or the Administrator revoking the authorisation;

c) by the User terminating the authorisation;

d) upon death of the User.

2.8 The User's access to the IEB shall be terminated no later than the end of the next working day following the date of receipt of the Account Owners' notice or termination of User's authorisation, unless a later date is specified therein.

2.9 If the legal entity as Account Owner undergoes a change in the function of a member of its statutory body who acted as a User, his User rights shall remain until the moment when a new User is set up, after the legal entity as Account Owner has given such an instruction to the Bank.

3 INTERNET AND ELECTRONIC BANKING SECURITY RULES

3.1 Terms and characteristics of personalised security features:

PIN for mobile app	A numeric code for the IB Mobile Apps that is used to activate, log in or authorise transactions.
Password for login	The password consists of numeric characters. It is used in IB Web Apps in combination with a one-time SMS code. The User is obliged to immediately change the initial password provided to the Users by the Bank.
Security Key (Smart Key, Business Key)	The function contained in the IB Mobile Apps is intended for logging in to the IB Apps or for authorising payment transactions and other requests or for generating one-time numerical codes for logging in or authorising transactions in the IB Web Apps even without connecting the device to the internet (so-called 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 IB 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 IB Web Apps.
Registered mobile telephone number	A telephone number notified by the User to the Bank that allows the user to receive one-time security codes, called SMS OTP (OTP stands for One-Time Password).
Registered e-mail address	An e-mail address notified by the User to the Bank that allows the User to receive one-time security codes (OTP e-mail).
Fingerprint (biometrics)	A fingerprint stored on the mobile device on which the IB Mobile App is activated.
Face scan (biometrics), Face ID	A face scan stored on the mobile device on which the IB Mobile App is activated. The face scan is compared with biometric data stored with the Bank or against the User's photograph (e.g., from an identification document).
Password (e.g., for communication with the bank, static password, access password, etc.)	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 IB Mobile App.
Username	An assigned or, in some cases, separately configurable username (alias) for logging in to the IEB App.
User number	A number assigned to the User by the Bank.
Identity document	A document issued by a public authority to the User, stating the name and surname, the date of birth and showing the appearance (e.g., ID card, driving licence, passport).
Birth certificate number	The birth certificate number assigned to the User.
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 personalised 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
Client certificate	A certificate used to authenticate (verify the identity of) a User. Allows confidential passive information (statements, balances, etc.) to be downloaded and decrypted into Eltrans 2000 (Gemini 5.0).
Electronic/Digital signature	Designation of specific data that replaces the classic handwritten signature or verified signature in the computer (applies to EB Apps)

3.2 In particular, 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, stolen, misused or used in an unauthorised manner. The User is obliged in particular:

a) To take appropriate measures to protect its personalised security features so that they cannot be lost, stolen, misused or used in an unauthorised manner.

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 IB Web Apps at https://cz.unicreditbanking.eu; https://cz.unicreditbanking.net and https://corporateportal.unicreditgroup.eu/container/cz/login

d) To keep passwords and PINs unmarked, 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 internet banking on a device unless the User is certain that no malicious program is installed on the device or unless the User has full control of the device (e.g., public internet cafes, computers shared by multiple people).

g) To give the password for communication with the Bank only to a UniCredit Bank employee in a situation where this password is required.

h) To protect SIM unlocking and use 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 User's 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/two-step authentication.

k) Not to allow an unauthorised person access to your mobile device (e.g., fingerprint, face scan, password, PIN).

l) If the User's mobile phone (or SIM card) is lost or stolen, to notify the Bank immediately and have the User's internet or electronic banking blocked as a precaution.

m) Not to allow the registration of biometric data of a stranger (or family members) on a mobile device.

n) To secure access to the User's mobile device with a password, PIN or biometric (fingerprint, face scan) and not to leave the User's mobile device unattended or automatically lock the User's device (screen) after a short period of time.

o) Not to use software modifications to the User's mobile device that allow full administrator access (e.g., jailbreak, root).

p) To regularly update the operating system of the User's mobile device and individual installed apps.

q) To use the latest version of security software (e.g., antivirus, firewall) on the User's mobile device.

r) Not to allow unnecessary permissions in a newly installed or updated app on the User's mobile device (e.g., access to SMS, facilitation, settings, 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 the User to install it, set the User's mobile device to prohibit the installation of apps from unknown sources.

t) Not to install apps based on someone else's instructions and, in particular, not to allow strangers to access the User's 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 User's operating system and the User's programs, especially the User's 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 User's computer from unauthorised access by setting access permissions, password security or other features. Not to allow a stranger remote access to the User's computer (e.g., via AnyDesk software).

y) To enter the Bank's website address manually. To access IB, use the Bank's website www.unicreditbank.cz, from there go to the IB login page, check that the User is accessing the relevant IB Web App website as defined in clause 3.3(c), and not to use a shortcut to the internet banking login page.

z) Not to access internet banking 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 the IEB Products 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.cz or unicreditgroup.cz, 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 the internet banking or to the mobile phone, in particular regarding fraud warnings.

3.4 If the Account Owner or User:

a) is a minor, the legal guardian is responsible for protecting the personalised security features and the safe use of the IEB Products;

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

4 LOGGING IN TO THE IEB APP, AUTHENTICATING, ACTIVATING THE IEB APP AND AUTHORISING A PAYMENT TRANSACTION, NON-PAYMENT ORDER OR SETUP INSTRUCTION

4.1 When logging in to the IEB App, the Bank authenticates the User through the appropriate combination of personalised security features listed in Chapter 3.

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

4.3 The Bank shall execute a payment transaction, non-payment order or setup instruction if it contains complete data conforming to the prescribed formats and is authorised in accordance with the relevant IEB App in accordance with these IEB Product 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 relevant conditions.

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

4.5 In the IB Mobile Apps, authorisation is carried out as follows:

a) by a fingerprint or by putting (scanning) your face to the device after the User is prompted to do so;

b) by entering a PIN when prompted to do so.

4.6 In the IB 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 for logging in to the IB Apps – the User receives a push notification in the Smart Banking App and then confirms the operation using biometrics (fingerprint or facial scan) or by entering a PIN;

(ii) Smart Key – an offline method for logging in to the IB Apps – the IB App displays a QR code on the login page, which the User scans via the Smart Key in the Smart Banking mobile app. The Smart Key generates a 6-digit one-time code, which the User enters into the Online Banking app and confirms;

(iii) Business Key – an offline method for logging in to the BusinessNet Professional, BusinessNet and 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 static password and then the Bank sends an SMS message to the User's designated mobile phone in the form of an SMS containing the OTP. The User enters this time-limited code back into the IB Web App to confirm the operation.

c) Hardware security key (token)
The password for signing an operation 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 IB Web App. The App then displays a 6-digit one-time code (OTP), which the User enters again in the IB Web App to confirm the operation.

4.7 Logging in to EB Apps can be done in one of the following ways: by entering a username and password, using an electronic/digital signature, or using a system username.

4.8 In the EB Apps, authorisation is using an electronic/digital signature based on a password entered in the client part of the app. The electronic/digital signature is used to sign and encrypt the data file, which can then be sent to the Bank for processing.

4.9 A payment transaction is cancelled in the same way as its authorisation, if the cancellation is enabled by the respective app.

4.10 In the IEB, the User can use the payment services of indirect payment order entry and the payment account information service.

4.11 The Bank is entitled to change the method of User's authentication, authorisation and other legal actions primarily for the purpose of enhanced security of the IEB Products. The Bank shall inform the User of the new authentication or authorisation method via the IEB app to which the change of authentication or authorisation method relates or in writing at least two months before the date on which the change is to take effect.

5 LIABILITY FOR UNAUTHORISED OR INCORRECTLY EXECUTED 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 or incorrectly executed 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 internet or electronic banking. The place for reporting is the Bank's Infoline, which is listed on the Bank's website in the Contacts section with 24/7- non stop availability or any branch during opening hours. The Bank also provides information on its website and at its points of sale on how the User is to report the loss, theft, misuse or unauthorised use of the personalised security features, the payment instrument or the IEB Product, including outside the opening hours of the Infoline and branches.

5.2 The Account Owner shall be liable for the loss of funds resulting from an unauthorised payment transaction up to an amount equivalent to EUR 50, if the loss was caused by the use of a lost or stolen payment instrument or personalised security feature or by the misuse of a payment instrument or personalised security feature, provided that the following conditions are simultaneously met:

a) the unauthorised payment transaction occurred before the User reported the loss, theft, misuse or unauthorised use of the payment instrument to the Bank; and

b) the User did not breach the duty to protect personalised security features intentionally or through gross negligence.

5.3 The Account Owner is liable for the loss of funds from an unauthorized payment transaction to the full extent if the User has caused such loss by fraudulent conduct or by intentionally or grossly negligently violating the obligation to protect their personalised security features.

5.4 The User shall be liable to the Bank for the damage arising in direct connection with a breach of its obligations under Article 3.

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 their defects, including infection, endanger or prevent the operation of the 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 Account Owner's or User's device or third party device used by them.

6.3 The Bank shall not be liable for the compatibility of the banking app with other app equipment on the 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 banking app. This shall be without prejudice to the regulation concerning exclusion or limitation of the Bank's liability pursuant to the General Business Terms and Conditions.

6.4 If the User is provided with access to product information provided by third parties through the IEB, 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:

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) 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.

6.6 In the event of a breach of a contractual obligation by the Bank, the Bank is liable only to the Account Owner and not to the person whose interest was to be served by the fulfilment of the agreed obligation.

7 INTERNET AND ELECTRONIC BANKING AVAILABILITY AND BLOCKING

7.1 The User may use the IEB Apps 365 days a year and 24 hours a day, unless the Bank does not allow access to the IEB 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 IEB 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 it is caused directly or indirectly by circumstances beyond the control of the Bank or its partners as a result of force majeure, natural disasters, hardware malfunctions, computer viruses or other events caused, for example, by a third party;

d) if the User logs in to the IEB from an IP address that shows suspicious activity (e.g., bulk sending of unsolicited commercial messages, chain messages, participation in hacking attacks, etc.)

7.2 The Bank is entitled to block all IEB Apps or User access (hereinafter referred to as the "Blocking"):

a) if the User or Account Owner violates contractual obligations in a serious manner or repeatedly;

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

c) if its 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/Account Owners in an appropriate manner about the execution of the Blocking made on the Bank's initiative before the Blocking is executed or immediately after the Blocking is executed, unless informing the relevant person would defeat the purpose of the Blocking or would be contrary to the law.

7.4 If the IEB App 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 ELECTRONIC BANKING

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

8.2 The Bank provides individual EB Products on the basis of ordered EB Products.

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

8.4 The initial date of use of the EB Product is the date on which:

a) the User has received from the Bank the installation media for the relevant EB Product and/or the certification and authentication tools in the case where the Bank provides the EB Product 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 EB Product by another licence rights owner;

c) the installation media for the system for the provision of the EB Products and/or the certification and authentication tools as ordered for the EB Products have been shipped;

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 at any time and the User is obliged to allow the Bank or a person authorised by the Bank to do so.

8.6 The Account Owner and the User agree to maintain the confidentiality of all messages received from the Bank, even after the end of the use of the IEB Products.

9 BANK IDENTITY

9.1 The Bank Identity is a means of electronic identification meeting the conditions of Act No. 21/1992 on banks, as amended (hereinafter referred to as the "Act on Banks"), and is used for remote identification of the client vis-à-vis the Bank, state authorities, authorities of self-governing local communities, as well as vis-à-vis third parties outside the framework of a qualified electronic identification system pursuant to Act No. 250/2017 on electronic identification, as amended (hereinafter referred to as the "Electronic Identification Act"), when using the services of these entities, should these entities and their technical capabilities so permit. The Bank is entitled to enable the use of the Bank Identity for the provision of trust services (including signing of documents) pursuant to Regulation (EU) No. 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market as amended. The Bank Identity consists of the identification data of the Client – a natural person in combination with personalised security features.

9.2 The Bank Identity is created on the day of its registration with the national point pursuant to the Electronic Identification Act (hereinafter referred to as the "National Point"). The Bank shall carry out this registration as soon as this is legally and technically possible.

9.3 The Client is entitled to prohibit the registration of the Bank Identity with the National Point in advance, or to prohibit the use of the Client's already registered Bank Identity. The Client is entitled to revoke such a prohibition at any time.

9.4 The Bank shall inform the Client about the registration of the Client's Bank Identity with the National Point. The Client is obliged to check the accuracy of the Client's identification data, which are part of the Bank Identity, immediately after learning of its registration.

9.5 The Bank Identity may be issued to the Client:

a) whose legal capacity has not been restricted;

b) who is more than 15 years old;

c) who has the relevant Product Contract concluded;

d) who has personalised security features in place to access IEB;

e) who has been identified in the manner laid down in point (b) of Section 38ac(1) of Act No. 21/1992 on banks, as amended; and

f) whose identity can be verified through the National Point by means of an identity card.

9.6 The Bank is entitled to cancel the Client's Bank Identity if it finds out that it was issued on the basis of false information, or if the Client's data becomes invalid and the Bank is not able to update them.

9.7 The Bank is entitled to update the Client's identification data on the basis of information received from the National Point.

9.8 The Bank Identity shall expire if the Client ceases to meet any of the conditions specified in Article.

10 FINAL PROVISIONS

10.1 The Client and the Bank derogate from the provisions of Sections 1799 and 1800 of the Civil Code on contracts concluded by adhesion. This excludes any invalidity of the provisions of these IEB Product Terms and Conditions or the relevant contract due to conflict with the aforementioned provisions on contracts concluded by adhesion in particular invalid clauses:

a) clauses that refer to terms and conditions outside the actual text of the relevant contract, the meaning of which has not been communicated to the Client, nor will it be proven that the Client knew their meaning;

b) invalid clauses that can only be read with particular difficulty or clauses that are incomprehensible to a person of average intelligence, even if they cause harm to the Client and their meaning has not been sufficiently explained to the Client; and

c) clauses that are particularly disadvantageous to the Client without reasonable cause, in particular if the relevant contract deviates seriously and without special reason from the usual terms and conditions agreed in similar cases.

10.2 The Client is entitled to terminate the contract at any time with a notice period of one month starting from the day following the date of delivery of the notice to the Bank or on a later date specified in the notice.

10.3 The Bank may terminate the contract in writing without giving any reason, effective at the end of the second calendar month following the month in which the notice was delivered to the Client, unless the Bank provides for a longer notice period.

10.4 The Bank shall be entitled to withdraw from the relevant contract in the event that the continuation of the obligations under the contract or the use of the IEB Product becomes unacceptable or illegal for the Bank due to the existence of applicable legislation or internal Bank policy.

10.5 The rights and obligations not regulated by these IEB Product Terms and Conditions are subject to the General Business Terms and Conditions of UniCredit Bank Czech Republic and Slovakia, a.s., the relevant product business terms and conditions for the agreed banking products and the relevant legislation.