GENERAL TERMS AND CONDITIONS FOR THE USE OF ELECTRONIC BANKING SYSTEMS FOR LEGAL ENTITIES, ENTREPRENEURS AND INDEPENDENT PROFESSIONAL OCCUPATION

I. Introductory provisions

By applying General Terms and Conditions for Use of Electronic Banking Systems (hereinafter referred to as: the General Terms and Conditions), UniCredit Banka Slovenija d.d. (hereinafter referred to as: the Bank) shall specify obligations, rights and conditions for use and operations through electronic and mobile banking systems. Individual terms specified below shall have the following meaning:

(1) **The Issuer** of General Terms and Conditions shall be UniCredit Banka Slovenija d.d., Ameriška ulica 2, 1000 Ljubljana, Slovenia, Swift designation BACXSI22, info@unicreditgroup.si, registered with the District Court of Ljubljana, commercial register number 1/10521/00, registration number 5446546. The Bank appears on the list of banks and savings banks, which have been granted a permit by the Bank of Slovenia to perform payment services. It is also published on the website of the Bank of Slovenia. The supervisory authority is the Bank of Slovenia.

(2) **The User** shall be a legal entity, an entrepreneur, an independent professional occupation, a community or a civil law entity, whom the Bank enables operations through electronic and/or mobile banking systems.

(3) **Statutory Representative of the User** shall be a private individual, who represents the User in accordance with the law and who is entered in the court register as a representative.

(4) **Authorized Person for use** (hereinafter: Authorized Person) shall be a private individual, who has legal capacity and who is empowered by the Statutory Representative of the User for the use of electronic and/or mobile banking systems by being stated on the banking form entitled User Authorization form for E-bank or User Authorization form for BusinessNet and Mobilna Banka PRO!. In case the Authorized Person is granted signing competence for his work with electronic and/or mobile banking systems, signature category shall be in accordance with banking form entitled Authorization for Disposal of Assets on Transaction Account.

(5) **Order form for electronic banking** shall be a bank form filled in by the User who wants to use electronic and/or mobile banking systems.

(6) **BusinessNet** shall be the online bank which is operable in an online browser and allows the User to carry out bank services.

(7) **Mobile bank PRO!** shall be a mobile application which works on mobile devices with the Android or iOS operating systems and allows the User to carry out certain bank services.

(8) **E-bank** shall be Halcom's solution for electronic banking which allows the User to carry out bank services.

(9) **Closed system** shall present the transaction between the User and the Bank on the basis of a special written agreement in accordance with Art. 1, par. 2 of ZEPEP. The closed systems in the Bank are: BusinessNet, Mobile bank PRO! and E-bank.

(10) **Personal security elements** shall be the personal properties ensured to the User by the Bank for authentication purposes and for electronic signing of payment orders, consents and orders to the Bank. They differ from each other based on the type of service and the type of the closed system, as follows: physical token, mobile token and personal password PIN. The personal security elements are also the qualified digital certificate or the certificate and PIN code, which are given to the User by certificate agency Halcom CA.

(11) **Authentication** shall be the process which allows the Bank to verify the identity of the User or the eligibility for using a certain payment instrument, including the usage of the User's personal security elements.

(12) **Strong authentication** of clients shall be an authentication with two or more elements which fall into the category of the User know-how (something that only the User knows), the User ownership (something which is exclusively owned by the User) and inseparable links with the User (something that only the User is), which are independent from each other, i.e. the violation of one element does not reduce the reliability of other elements, and are designed in such a way as to protect the confidentiality of the data being verified.

(13) **Physical token** shall be an electronic device which is protected with a 4-slot personal password and generates time barred one-time numeric passwords which uniquely determine the authentication of the Authorized Person in the online bank.

The one-time numeric password from the token, together with the username which the Authorised Person sets themselves, ensures a unique authentication of the Authorized Person when logging into the BusinessNet system and during the process of electronic signing. The usage of the token is limited to only one User. Strong authentication in online banking demands from the User at physical token an additional generation of a time barred, one-time password for signatures (OTP), with which the User confirms the implementation of the transaction or consent together with the summary of the transaction or consent to the Bank.

(14) **Mobile Token** shall be a software which is an integral part of the application Mobilna banka PRO! or a standalone application and generate time barred onetime numeric passwords that uniquely determine the authentication of the Authorized Person of the Mobilna banka PRO! and BusinessNet systems. The Mobile Token, together with the personal password PIN which the Authorized Person sets themselves, ensures a unique authentication of the Authorized Person when logging into the system Mobilna banka PRO! and BusinessNet and during electronic signing.

(15) **Personal password PIN** (hereinafter: PIN) shall be a secret personal identification number chosen by the Authorized Person themselves and which consists of a sequence of numbers, with which the Authorized Person may identify themselves at the entry or electronic signing in online and/or mobile banking. The PIN must not have less than 6 or more than 8 numbers. An unsuccessful login is possible three times; after the third unsuccessful attempt, the online/mobile bank is automatically locked. In order to unlock the online/mobile bank, the contact centre of the Bank must be contacted. If the PIN number is incorrectly entered three times at the Mobile Token, then the wrong security flag is shown, which communicates to the User that they have entered an incorrect personal password.

(16) **The fingerprint and face ID** (the Face ID on iOS devices) are biometric identifiers of the User and may be used instead of the personal password or PIN to enter the Mobile Bank PRO!, to sign payment orders in the Mobile bank PRO!, and to sign online transactions by means of the Mobile Bank PRO!

The modules for the authentication of your fingerprints or face recognition in your device are not provided by the Bank. Your fingerprint or face are stored in your mobile device. The Bank does not process (save or access) the data on the fingerprint and face image; therefore the Bank is not the controller of such personal data. Also, it cannot be deemed that a contractual data processor processes such kind of data on behalf of the Bank. According to this, the Bank does not provide for the compliance of processing such kind of personal data in accordance with the Personal Data Protection Act (ZVOP-2) or the General Data Protection Regulation (GDPR). The Bank is not responsible nor liable for the security of the fingerprint and face recognition function on any device, nor for the performance of the function in the manner presented by the producer of the device.

Consider the necessary security measures to protect your mobile device and do not save fingerprints and face images of other persons on your mobile device. Handle your mobile device carefully and responsibly to protect it from loss, theft or unauthorised use.

(17) **Activation code** shall be a one-time and time barred code sent by the system and which serves as an activation for mobile banking and mobile token services. Following a successful activation, the Activation code becomes unusable for any further use. The Activation code also becomes unusable if the User fails to activate the application within 72 hours of receiving the code.

(18) **One-time numeric password** shall serve as the verification of the synchronisation between the token and the back system, and shall be generated following the entry of the personal password PIN into the token. It consists of 6 digits and is time barred. Such a password may only be used once. An unsuccessful login is possible three times; after the third unsuccessful attempt, action of a bank employee is necessary.

(19) **Username** shall be a one-time string of alphanumerical characters with which the Authorized Person identifies themselves when entering the application Mobile bank PRO! or BusinessNet.

(20) **Qualified digital Certificate** (hereinafter referred to as: the Certificate) shall be the Authorized Person's public digital key, which is signed by certification authority of digital Certificates (Halcom CA – Certificate agency) together with the Authorized Person's personal data.

(21) **Smartcard** shall be a security instrument containing the Certificate, which serves for the purposes of authentication and electronic signing.

(22) **Smartcard reader** shall be a device, which reads the Smartcard and which the Authorized Person needs for smooth operating activities through E-bank.

(23) **Smart PKI USB key** shall be a security instrument containing the Certificate, which serves for the purposes of authentication and electronic signing (a substitute for the Smartcard and the Smartcard reader).

(24) **PIN code or personal number** shall be a sequence of characters, which enables safe use of E-bank together with the Smartcard or the PKI USB key; The User or the Authorized Person for Use of E-bank shall receive his PIN code from Halcom CA; after three false entries of the PIN code, the Smartcard or the PKI USB key shall automatically lock.

(25) **PUK code** shall be the number used for unlocking of the Smartcard or the PKI USB key, which the User or the Authorized Person for Use receives from Halcom CA.

(26) **Halcom CA** shall be the certificate agency producing Qualified Digital Certificates as well as the PIN and PUK codes for users of E-bank (hereinafter referred to as: the Certificate Provider).

(27) **Debit Account** shall be a transaction account, which is stated on a payment order that has been sent for payment as an account number for debit.

(28) **File Exchange** (in suitable structure) shall be a file exchange in formats, which the Bank and the User agree upon beforehand in writing.

(29) **Electronic signature** shall be a string of data in electronic form which is included, added or logically linked to other data (e.g. electronic document) and is meant to verify the authenticity of such data and the identification of the signatory. The electronic signature replaces the handwritten signature and has the same evidential value as the handwritten signature.

(30) **The Signatory** shall be the Authorized Person for working in the systems of electronic and/or mobile banking, who has the authorization of signing and who creates an electronic signature.

(31) **Daily limit** shall be the highest allowed amount of the sum of outflow transactions in one day.

(32) **Transaction limit** shall be the highest allowed amount of each outflow transaction.

(33) **E-invoice** shall be an invoice issued in standard electronic form and equally substitutes paper form of the invoice that the issuer of the invoice transmits to the recipient of the invoice for the service / goods delivered, etc. The E-invoice is in compliance with the legal regulations governing this area. As an E-invoice, in these General Terms and Conditions, all E-documents related to the E-invoice are also considered:

E-payment notice, E-debit note, E-credit note, E-purchase order, E-dispatch advice, E-proforma invoice.

(34) **The E-invoicing system** enables smooth and successful exchange of E-invoices to all participants: issuers, recipients, intermediaries and archivists.

(35) **Central processor** is an intermediary which is responsible for the transmission of E-invoices between individual banks, namely the participants of the E-invoice system.

(36) **E-invoice Issuer** is a legal entity that has a business relationship with the E-invoice recipient, on the basis of which the E-invoice is issued to the recipient.

(37) **E-invoice Recipient** is a private individual, an individual proprietor, an entrepreneur or a legal entity who has a transaction account with the bank and is a user of an electronic bank, and has a business relationship with the E-invoice Issuer.

(38) **E-invoice Service** is a service which enables the Bank to transfer invoices of an E-invoice Issuer in the e-form into the electronic bank and thus enables E-invoice Recipients to receive E-invoices.

(39) **E-registration** is electronic form of registration for receiving an E-invoice, made by the user via an electronic bank. It is sent via the system to the E-invoice Issuer, which is indicated in the E-registration. The user makes the E-registration for each E-invoice Issuer separately.

(40) **E-deregistration** is electronic form of deregistration from the receipt of an E-invoice, made by the user via an electronic bank. It is sent via the system to the E-invoice Issuer, which is indicated in the E-deregistration. The user makes the E-deregistration for each E-invoice Issuer separately.

(41) **The order** is a request for the execution of a banking service, which the user sends to the Bank using the electronic or mobile bank after successful authentication and electronic signing.

(42) **Manual** is the document containing a technical description and specifications of the E-invoice. It has been issued by Halcom d.d. and published on its web page www.halcom.si.

(43) **Instant payment** – a domestic or cross-border credit payment in euros with immediate settlement and approval of the payee's account.

(44) **Verification of Payee (VoP)** – a security feature that verifies the match between the first and last name or title of the payee entered by the payer in the payment order and the first and last name or title of the account holder to whom the payment is being made.

II. Protection of personal data and confidential information

(1) The Bank is the controller of personal and other confidential data of the User (and Authorized Persons), which is acquired in establishing a business relationship and continued operation with the User (or Authorized Person).

(2) For the purpose of performing mutual contractual relations and the purposes of marketing, the Bank processes, keeps, transmits and protects personal and other confidential data in accordance with the law governing the protection of personal data, the EU General Data Protection Regulation (Regulation (EU) 2016/679-GDPR), the law governing banking, the law governing commercial companies and other regulations relating to the protection of personal and confidential data and business secret and in accordance with its internal acts.

(3) More detailed information, the rights of individuals relating to the processing of personal data and contact details are set out in the General Information on the Processing of Personal Data. General Information on the Processing of Personal Data in force at the relevant times is available at the Bank's premises and on its website (www.unicreditbank.si).

(4) The User (and/or Authorized persons) and associated Users (and/or Authorized persons) are acquainted with and agree that the Bank can save a copy of their personal ID in electronic form to the place where other documents on individual User are saved and to all places where documents on all connected Users are electronically saved.

III. Main features of electronic and mobile banking systems

(1) The User and the Bank shall agree that within electronic and/or mobile banking system an individual device, which is or contains the means for authentication together with associated code for use, is considered to be a payment instrument.

(2) **BusinessNet** enables high level of safety by use of the PIN time dependent Token for generating Passwords, data transfer Certificate and Username.

The valid daily and transaction limit in BusinessNet are determined by the Bank. The daily limit for each account for entrepreneurs and small companies is EUR 1 million, and EUR 10 million for large companies. The highest allowed transaction limit is equal to the daily limit. Limits are established at the activation of BusinessNet and can be changed only at the User's request.

BusinessNet can also be used on mobile and other devices (GSM phones, smart phones, , tablet PCs, etc.; hereinafter referred to as mobile devices), where the operating system and browser enables access to the internet. Due to technical limitations of individual types of mobile devices, some BusinessNet functionalities on such mobile devices are not enabled, or the execution of the individual functionality is suitably adapted and limited.

If the Authorized Person for BusinessNet also accesses to use of mobile banking, until revocation or amendment its existing user authority shall apply on all accounts on which he is authorized with his username in BusinessNet, reduced in accordance with the limitations and characteristics of the mobile bank. The characteristics and limitations of the mobile bank are available on the website of the Bank https://www.unicreditbank.si/si/podjetniki-in-mala-podjetja/digitalno-bancnistvo-za-podjetnike/mobilna-banka-pro.html and are subject to change.

(3) **E-bank** excels at extreme reliability, simplicity of installation and use, and state-of-the-art protection by means of the PKI (Public Key Infrastructure) technology.

The valid daily and transaction limit in E-bank are determined by the Bank. The daily limit for each account for entrepreneurs and small companies is EUR 1 million, and EUR 10 million for large companies. The highest allowed transaction limit is equal to the daily limit. Limits are established at the activation of E-bank and can be changed only at the User's request.

(4) Electronic banking systems enable the User the application of the following services:

a. Pursuit of payment services,

b. Monitoring of bookkeeping balance and current outstanding on transaction account,

c. Monitoring of transactions on notified accounts,

d. Receiving and sending messages between the User and the Bank,

e. Other electronic services, which are described in product presentations for an individual client segment.

(5) **Mobilna banka PRO!** is a mobile banking program that enables the user insight and performing banking services in BusinessNet. The Authorized Person shall install the program in mobile device via App Store or Google Play online store. The application shall be activated by the activation code, which is also received via SMS (hereinafter referred to as: mobile bank). The mobile device on which the program is installed must enable internet connection to use mobile bank. With the use of mobile token and personal PIN code the mobile bank provides sophisticated security mechanisms and a high level of data encryption. Access to financial data and mobile banking functionality is not possible without the personal PIN code, which is known only to the user. Additional security is ensured so that the data in connection with the user's bank accounts are never stored on the mobile device as well as with a time limit access to application which is closed automatically after three minutes of inactivity and is automatically locked after three consecutive incorrect entries of personal PIN code.

(6) The existing authorizations of Authorized Person are valid upon accession to use of the mobile bank to cancellation for all accounts on which he is authorized in BusinessNet or they are reduced in accordance with the limitations and characteristics of the mobile bank. The characteristics and limitations of the mobile bank are available on the website of the Bank https://www.unicreditbank.si/si/podjetniki-in-mala-podjetja/digitalno-bancnistvo-za-podjetnike/mobilna-banka-pro.html and are subject to change.

The valid daily and transaction limit in the mobile bank are determined by the Bank and can be changed by the user within the mobile bank application. The daily limit for each individual account in the mobile bank is equal to the daily limit in the online bank BusinessNet. If the lower transaction limit is set by the Bank in BusinessNet upon activation, then the mobile bank considers the lower limit.

(7) The access to Halcom E-Bank, BusinessNet and application Mobilna banka PRO! is not permitted from Iran, Syria, North Korea and the following regions in Ukraine: Crimea, Sevastopol, Donetsk, Lugansk, Kherson, Zaporozhye as a subject of restrictive measures imposed against them.

IV. Method and means of communication

(1) To be able to apply electronic banking systems, the User shall ensure appropriate computer (hardware and software) or mobile device and communication equipment, which is specified in Technical Requirements for an Individual System. Applicable Technical Requirements for an Individual System are available on the Bank's website https://www.unicreditbank.si/si/podjetniki-in-mala-podjetja/digitalno-bancnistvo-za-podjetnike/e-bank.html#dokumentacijainobrazci and represent the mandatory instructions to users about the way and adequacy of using of electronic and mobile banking, and other relevant guidance on the use of electronic and mobile banking.

(2) Electronic and mobile banking systems are closed systems. Documents, which the Bank forwards to the User or the Authorized Person via electronic or mobile banking systems, shall be equivalent to paper documents, which the Bank sends via post and which can be replaced by electronic ones.

(3) Mobile bank enables to the User and Authorized Person to review sent orders that were generated in the mobile bank within the menu Archive of payments. On the basis of the User order which is sent through electronic banking systems or in business unit of the Bank, the Bank shall send to the user all transactions conducted through mobile bank on paper or another permanent data carrier.

(4) All data, which the User can receive from the Bank in electronic form, shall be sent to the User by the Bank in paper form only upon the User's special request and upon payment of a fee determined by the Bank's price list.

(5) The Bank shall enable the User and the Authorized Person saving and printing of sent data so that they are available to them for later use within a period appropriate for the purpose of the data, and enable them unmodified viewing of saved data.

(6) If the User does not want to continue using the online bank BusinessNet, then the User is obligated to transfer and save onto a permanent data carrier all the electronic documents in the menu Messages and the menu Statements before closure, in order to preserve such data in electronic form for later use.

(7) A Certificate shall be the means of authentication when using the E-bank system. It is a public key of the Authorized Person, which is signed by the certification authority of digital certificates (certificate agency) together with the Authorized Person's personal data. A Digital Certificate shall enable identification of the Authorized Person, implementation of signature of digital documents and protection of confidential data transfer by means of encryption.

(8) A safety instrument holding a Certificate may be a Smart PKI USB key or a Smartcard. In case the Authorized Person uses a Smartcard, he shall have a Smartcard reader, which reads the Smartcard and which the Authorized Person needs for smooth operating activities via E-

bank program. If the Authorized Person applies the Smart PKI USB key, the Smartcard reader is not required.

(9) The Authorized Person shall receive the PIN and PUK codes from Halcom CA. The PIN code consists of a sequence of characters, which, together with the Smartcard or the PKI USB key, enables safe use of E-bank and authentication of the Authorized Person. After three false entries of the

PIN code, the Smartcard or the PKI USB key shall automatically lock. It shall be necessary to apply the PUK code to unlock the instrument.

(10) When entering the E-bank program, the Authorized Person shall log in by means of a security instrument (the Smartcard in combination with the Smartcard reader or the PKI USB key) and a PIN code.

(11) The PIN code shall be entered to receive or send data. When data are sent and the PIN code is entered and confirmed, it shall not be possible to stop the process of sending. In case of three false entries, the instrument shall lock for safety reasons. The User shall handle the Certificate and personal numbers (PIN and PUK) with utmost care and protect them with due diligence to prevent loss, theft and/or abuse. He shall ensure equivalent keeping and protection also with his Authorized Persons.

(12) The User or the Authorized Person shall agree for the Bank to notify him via electronic and/or mobile banking systems about all modifications, novelties in its offer and specialties regarding its business operations. The Bank's notifications regarding its offer are specially marked for users.

V. Acquisition of electronic and/or mobile banking systems

(1) The Bank shall grant the use of the electronic and/or mobile banking system to the User if he:

a. Forwards to the Bank duly completed all the necessary originals of bank forms,

b. Has a bank account with the Bank,

c. His operations on his transaction account are upright,

d. Regularly meets his obligations,

e. Has already acquired and completed at least one means of authentication the Bank recognizes.

(2) The Bank shall reserve the right to reject the User's request without giving reasons. The Bank shall so notify the User in writing.

(3) One or more Authorized Persons may be authorized for use by the User's Statutory Representative. He shall specify the type of authorization for an individual Authorized Person in a suitable bank form. The Bank shall include the Authorized Person when it receives a duly completed bank form.

(4) To use electronic and/or mobile banking systems, the User may order with the Bank a modification for adding or blocking authorization of individual Authorized Person on the means of authentication by means of a suitable bank form.

(5) In case the Authorized Person is granted electronic signing competence for his work with electronic and/or mobile bank, Authorized Person's data shall be in accordance with the data on a banking form entitled Authorization for Disposal of Assets on Transaction Account of the User.

(6) The Bank shall grant to the User of BusinessNet the order and use of Mobile bank PRO! on the basis of the User's order through electronic bank - BusinessNet or by filling out an application for the use of electronic and/or mobile banking system in any of business units of the Bank.

(7) The order and activation of a service is a prerequisite for using the service.

(8) The activation code is no longer useful, if the application is not activated by the User within 72 hours upon receipt of an activation code.

(9) It is considered that the agreement shall apply from the date the Bank approves the use of BusinessNet service or Mobile bank PRO!.

(10) To add or replace the Certification Instrument in E-bank, the User shall attach a completed and signed document entitled Written Confirmation of Identity of a Digital Certificate for the Authorized Person.

(11) With the signature the User confirms that he accepts the valid General Terms and Conditions.

VI. Acquisition of assets for authentication and electronic signing

(1) Acquisition of the physical BusinessNet Token

The User shall order the physical Token at the Bank. When accepting the Token, the Authorized Person and the User shall assume full responsibility for the Token and acts resulting from an action in BusinessNet. The physical Token is owned by the Bank, which hires it out to the User for the time of his use of BusinessNet and has 1 year warranty. The warranty does not apply in case of damage or physical interference in a Token.

(2) Acquisition of Mobilna banka PRO!

In case of order and signed contract for mobile banking service the User or Authorized Person of mobile bank shall receive also Mobile Token at the acceptance of application (Mobile Token is an integral part of the application). The Mobile Token, together with the personal password PIN, uniquely authenticates the Authorized Person in mobile bank. (3) Acquisition of Certificate for E-bank system

The User may order a Certificate for the Authorized Person either at the Bank or directly at the Halcom CA certificate agency. The Bank shall perform registration service under regulations of the digital certificate provider, who publishes existing policy of certificate agency on its website.

(4) In case the User wishes to install:

a. a network, multi-user version of Corporate-E-bank (which enables co-
access to database to all Authorized Persons authorized for the access to electronic bank) or

b. an upgraded, network version B2B-E-bank (which enables a direct automatic document exchange between the company's information system and that of the Bank),

the admission process shall be the same, except that in this case it is necessary to arrange a meeting with the producer of the program – Halcom d.d. to install the program.

(5) Halcom d.d. shall install Corporate/E-bank or B2B/E-bank versions under its own conditions and price list, independently of the Bank.

VII. Exchange of E-documents procedures

(1) With a view to the application of the E-invoice Service, the following standardized document types can be exchanged via the electronic bank:

a. **Envelope** is the basic document which travels via the System and which plays a similar role in the electronic world as a paper container for a letter in the paper world. The Envelope contains data for directing and the preparation of payment, the digitally signed E-invoice and any supplements;

b. **Supplement to Envelope** is an E-invoice in accordance with the E-style standard in the XML form and an edited form of an E-invoice in the PDF/A form;

c. **E-registration/E-deregistration** are consents or a registra- tion/ deregistration enabling/disabling the receiving of E-invoices; they are in the electronic form;

d. Feedback for E-registrations.

(2) The Bank shall be obliged to ensure a business partner all the required documentation which describes the scheme of an individual document type. Standards concerning the exchange of an E-invoice and an Envelope are defined in the Manual. The business partner shall ensure that they are acquainted with the contents of the Manual and to strictly take into account provisions of the applicable Manual. The Bank shall inform business partners about any changes in due time.

(3) To be able to use the E-invoice Service, business partners as Issuers shall:

a. Have a transaction account with the Bank,

b. Conclude the Agreement on the Use of the E-bank Electronic Bank with the Bank,

c. Conclude an agreement on the use of the E-invoice Service with the Bank,

d. Use the version of the E-bank electronic bank by the recommendations of the Bank,

e. Authorize at least one authorized representative with a valid qualified certificate for the use of the E-invoice Service.

(4) The Bank shall not deliver an E-invoice to the Recipient if:

a. The E-invoice and its supplements do not comply with provisions of
these General Terms and Conditions and the Manual,

b. The Recipient does not have a transaction account,

c. The Recipient does not have a transaction account included in the electronic bank,

d. The Recipient and a business partner do not agree on the receipt of E-invoices,

e. The Recipient's bank does not enable the receipt of E-invoices.

(5) Requirements concerning electronically issued invoices are analogous to a written form of invoices and are prescribed by the Value Added Tax Act (ZDDV - 1), namely by Articles 81 and 82 of the ZDDV - 1. Taxable persons referred to in Article 81(6) of the ZDDV – 1 shall be required to also take into account Article 75(a) of the Rules on the Implementation of the Value Added Tax Act (the Official Gazette of the RS, No.79/02 and 114/02).

VIII. Implementation of payment orders

(1) It shall be considered that the Bank has received a payment order when one or more Authorized Persons (in compliance with authorizations on the account) sign and send the order through electronic and/or mobile banking systems to the Bank's server. The Bank shall notify the User about order implementation process by means of feedback via electronic and/or mobile banking systems.

(2) The Bank shall assure the User realization of all duly completed payment orders within time-limits prescribed or agreed upon for individual type of an order in accordance with Payment Transactions Business Hours (hereinafter referred to as: Business Hours). If the User or Authorized Person decides to cancel processing of a payment order, he may communicate it to the Bank in a correct manner through electronic and/ or mobile banking in line with the Business Hours.

(3) An instant payment order shall be processed within 10 seconds from the moment the payment order is deemed to have been received, in accordance with the General Terms and Conditions of Keeping Transaction Accounts and Pursuing Payment Services for Legal Entities, Entrepreneurs and Independent Professional Occupations.

(4) A payment order dated on a specific day shall be deemed to have been received by the bank on the day specified in the payment order. If that day is not a business day for the bank, it shall be deemed to have been received on the next business day.

IX. Blocking or termination of use of electronic and/or mobile banking systems

(1) The User may terminate his contract in writing, with immediate effect, at any time and with the agreement of the Bank. The User may unilaterally terminate the contract in writing at any time by giving 15 days' notice. The User shall forward his proposal for termination of use of electronic and/or mobile banking system to the Bank on a suitable bank form.

(2) The Bank may, at its own discretion and unilaterally, temporarily or permanently disable the use of electronic and/or mobile banking systems for the user and/or authorized representative without a specified deadline and without any compensation or other obligations. The bank shall notify the user and/or authorized representative of such a decision as soon as possible.

The Bank may, at its own discretion and unilaterally, without a specified deadline and without any compensation or other obligations, also terminate the contract on the use of electronic and/or mobile banking systems in writing and exclude the user and/or authorized person from the system.

(3) As of the termination date, the Bank shall block the use of the package software and clear all the User's outstanding liabilities according to the price list.

(4) All orders, which have been sent to the Bank prior to termination of use, shall be realized if all terms under which the Bank ensures realization are complied with.

(5) Upon the User's request, the Bank may block the existing means of authentication for his Authorized Persons on accounts by means of a form entitled Competences of the Authorized Person of the System and charge the service in accordance with its applicable price list.

(6) The Bank may effect blocking/cancellation of the User on the basis of a completed bank form entitled "Application for cancellation or blocking

of electronic banking." In this case, all the User's competences are blocked/cancelled only on accounts, which are stated on the form.

(7) The Bank shall automatically block the use of the mobile banking application after three consecutive incorrect entries of personal password PIN by the Authorized Person.

(8) All forms shall be in original and shall be signed by the Statutory Representative of the User and his bank consultant.

(9) The User must immediately notify the Bank or other security service, which has issued the instrument, about any loss, theft or risk of abuse of the means of authentication for electronic and/or mobile banking systems (the BusinessNet Token, mobile phone for Mobile bank PRO!, Halcom's Qualified Digital Certificate for the E-bank system). In case of a mobile banking system User, it shall immediately notify about loss or theft of mobile phone also its mobile operator.

(10) In accordance with an individual system, the Statutory Representative, a company officer with statutory authority or the User himself may send the Application for Blocking:

E-bank, BusinessNet and/or Mobile bank PRO!:

a. every working day via phone +386 1 5876 930 between 7.00 am and 6.00 pm

b. at any time via e-mail (email: blokada.zloraba@unicreditgroup.si)

E-bank:

a. Blocking of the means of authentication is possible 24/7 via the provider Halcom CA. Blocking procedure can be found on the provider's website. When the Instrument is blocked by the provider Halcom CA, it is also blocked by the Bank.

(11) The person canceling the use, shall be liable for authenticity of provided data. After receiving the message, the Bank shall prevent the possibility of sending payment orders via electronic and/or mobile banking systems, or shall block or withdraw certain authorizations for use of electronic and/or mobile banking system from an individual Authorized Person.

(12) Within a Business Day the Statutory Representative shall forward to the Bank in writing the original of the completed bank form about blocking of the electronic banking system of the User and/or the Authorized Person. It shall be signed by the Statutory Representative and his bank consultant otherwise the Bank shall return to the status as it was prior to blocking.

(13) The Bank shall be liable only for unlawfulness on the side of the Bank and shall not assume strict liability for damage incurred prior to receiving the Application for Blocking.

(14) The Bank shall consider orders, which the Authorized Person has sent to the Bank prior to termination of his authorizations, as correct.

(15) Costs of either a new Token or Halcom's Digital Certificate shall be charged to the User.

(16) Unblocking may be effected at any time on the basis of an official letter provided by the Statutory Representative.

X. Obligations of the User and the Authorized Person

(1) The User shall commit himself to:

a. Safeguard the means of authentication and use it only for operations envisaged for the use of electronic and/or mobile banking systems;

b. To handle his means of authentication, personal numbers (PIN and PUK), the medium holding his electronic signature, Username and Passwords with utmost care and protect them with due diligence to prevent loss, theft and/or abuse, and to ensure equivalent keeping and protection also with his Authorized Persons;

c. Regularly receive and send data;

d. Regularly receive and check notices sent by the Bank;

e. Follow instructions for use of electronic and/or mobile banking systems and applicable law;

f. Immediately notify the Bank about all ascertained irregularities or atypical functioning of electronic and/or mobile banking systems;

g. Immediately notify the Bank about a modification or termination of an individual Authorized Person's validity of authorizations;

h. Immediately notify the Bank about any unauthorized use, suspected unauthorized use or the possibility of unauthorized use or any other abuse or suspected abuse or the possibility of abuse and to forward the Bank a request for blocking in writing;

i. Periodically ensure valid Digital Certificates of his Authorized Persons by providing replacement or renewal in due time prior to actual expiry;

j. Keep a register of his Authorized Persons and their competences; k. Take into account instructions concerning E-invoices in the Manual;

l. Correctly form the standardized Envelope and E-invoice in accordance with the Manual;

m. Send Recipients in an individual Envelope the maximum of one E- invoice in accordance with the E-style standard in the XML form and the maximum one edited form of an E-invoice in the PDF/A form;

n. Send their Recipients via the System only contents which are directly linked with the E-invoice and not to send advertising contents as a supplement to the E-invoice,

o. Receive E-registrations/E-deregistration of private individuals and legal entities and include these entities in/exclude them from their register of E-invoice Recipients on the basis of these E-registrations/
E-de-registrations,

p. Enable E-registration/E-deregistration for the receipt of E-invoices also via their web portals and make the arrangements for incorporating these data into their register,

q. Manage their up-to-date register of E-invoice Recipients.

(2) The Authorized Person shall commit himself to:

a. Safeguard his Qualified Digital Certificate, personal numbers (PIN and PUK), the medium holding electronic signature, Username and Password with due diligence to prevent damage or disposal as defined in case of the User;

b. Not to put down personal Passwords, Usernames and PIN numbers onto paper or electronic media;

c. Renew his personal number (PIN) at least once a month;

d. Notify Certificate owner (legal entity to whom Certificate is issued) and acquire his permission if he wishes to add a Certificate onto a transaction account of another legal entity; the Authorized Person himself shall be held responsible for authorizing a Certificate onto another legal entity.

(3) In case of destruction, disposal or loss of the means of authentication, all costs of manufacture of a new one shall be paid by the User.

XI. Verification of Payee

(1) Verification of payee is an additional security service that allows the payer to check whether the name or title of the recipient entered matches the IBAN number and the name or title of the recipient at the recipient's bank. Recipient verification is performed before the payer confirms the payment order. Based on the verification, the payer receives one of the following notifications:

Perfect match – The entered recipient information corresponds to the data associated with the IBAN at the recipient's bank.

Partial match – a minor discrepancy has occurred with the records of the recipient's name or title. The payer simultaneously receives information about the correct or full name of the recipient with a notification of the match.

No match – The entered name or title does not match the name or title of the recipient associated with the entered IBAN.

Valuation of payee is out of services at the moment – The system is currently unable to verify the recipient for the specified IBAN.

(2) The payer can only confirm the execution of the payment order after receiving notification of a match, partial match, or no match.

(3) In the Halcom E-Banka application, after the execution of the VoP service, the user does not receive a special notification in the event of a complete match of the beneficiary's data. The user of the Halcom E-Banka application may choose not to use the beneficiary verification service for the execution of a bulk payment. The user may later, at any time, decide to re-enable the beneficiary verification service for bulk payments. After 90 days from deactivation, the service is automatically reactivated.

(4) In the BusinessNet application, the VoP service is not performed at the level of the bulk payment package. Instead, the user has the option to verify the beneficiary's data for each individual payment order within the payment package. This is done by opening the content of the payment package, selecting the individual transaction, reopening it, and saving it again, whereby the beneficiary verification service is performed for the selected payment.

XII. Responsibility of the Bank

(1) Upon accession to use of electronic and/or mobile banking systems, the Bank shall ensure all the necessary elements for use of electronic and/ or mobile banking systems to the User and the Authorized Person.

(2) The Bank shall ensure the User and the Authorized Person continuous use of the electronic and/or mobile banking system. However, exemptions should apply to failures due to cases of force majeure, technical problems, other unexpected failures and failures during preannounced suspensions of system operation.

(3) The Bank shall not be responsible for damage incurred due to emergency situations and events such as cases of force majeure, strikes, decisions and actions of bodies of authority, functional disturbances in telecommunication and other traffic, errors incurred at data transfer via telecommunication networks, and denied access to services of electronic and/or mobile banking systems.

(4) The Bank shall not be responsible for any damage incurred to the User or the Authorized Person under the head of non-functioning of electronic and/or mobile banking systems or the entire computer system, which would be caused by ineligible interventions of the User or third parties.

(5) The Bank shall be liable to the User or the Authorized Person for the damage incurred by the Bank deliberately or as a result of serious negligence. The Bank shall be liable only for directly incurred damage. In case the User or the Authorized Person detects a failure, an irregularity or in case damage is incurred, he shall act in accordance with these General Terms and Conditions.

(6) The Bank shall not undertake responsibility in case of loss or damage of data and equipment of the User or the Authorized Person due to installation and use of the electronic and/or mobile banking system.

(7) The Bank shall not be responsible for any damage in cases when the User does not keep his own record of Authorized Persons, their payment instruments or their competences on his accounts.

(8) Furthermore, the Bank shall not be responsible if the User does not keep his own record of his Authorized Persons, their Digital Certificates and their competences.

(9) Also, the Bank shall not be responsible if the Authorized Person authorizes the Certificate to a transaction account of another legal entity other than the Certificate owner.

(10) The Bank shall accept all adequate e-documents which have been prepared and sent by a business partner.

(11) The Bank shall accept the received E-invoices into its System and submits them to Recipients in the electronic bank or the Central processor no later than within 2 business days after it received them from a bank.

(12) The Bank shall reject E-invoices in a wrong format and inform the business partner thereof no later than within 2 business days.

(13) The Bank directs E-invoices for Recipients within the Bank into the electronic bank system and submits feedback to the business partner concerning successfully delivered E-invoices if the business partner requires such information in the Envelope.

(14) The Bank submits E-invoices for Recipients of E-invoices in other banks via the Central processor if this is possible at a certain point in time.

(15) The Bank shall make an E-invoice available to the Recipient at the accessible place, which has been agreed upon.

(16) The Bank shall reject E-invoices if they contain incorrect data or unsuitable contents.

(17) The Bank shall make information about Issuers available to Recipients of E-invoices at the place, which has been agreed upon.

(18) The Bank shall enable the sending and receiving of E-registrations and E-deregistrations.

(19) The Bank shall enable the sending and processing of an E-advice of delivery as a reply to an E-registration or E-deregistration.

(20) In the event that the payer confirms the execution of the payment despite receiving a notification of a mismatch, the bank is not liable for executing the payment to an unintended recipient of the payment based on the unique identification code.

XIII. Fees

(1) The Bank shall charge the User fees for the use of electronic and/or mobile banking services in the amount, within time-limits and in the manner determined by its applicable price list.

In case of destruction, disposal or loss of the means of authentication, all costs of manufacture of a new Instrument shall be paid by the User.

XIV. Amicable settlement of dispute

(1) The User and the Bank shall resolve any disputes, disagreements or complaints with regard to supplying of services consensually in accordance with these General Terms and Conditions.

(2) The Bank shall resolve any disputes and disagreements based on a written or oral complaint of the User. The User may submit a written complaint at any Bank branch, send it to UniCredit Bank Slovenija d.d. Ameriška ulica 2, 1000 Ljubljana (with the indication Complaint Monitoring), via electronic banking (BusinessNet or E-bank), via e-mail to the competent contact person at the Bank's branch, to the Bank's e-mail address info@unicreditgroup.si or via the web portal https://www.unicreditbank.si/si/prebivalstvo/application-forms/obrazec-povratne-informacije.html. The User may submit an oral complaint in person or by telephone at any Bank branch or by contacting the Bank contact centre at 01 5876 930. The Bank shall only be obliged to reply to complaints submitted in writing.

A complaint should be fully clear and comprehensible and should contain a description of the facts that are the object of the complaint. It should include the following:

- Data on the complaining party (name, surname, address, e-mail address, telephone or title and registered office of the legal person or holder of activity);
- A description of the grounds for the complaint and the event or an indication of the key facts and the date of the event;
- An indication of documents the complaint relates to;
- The submission of evidence confirming the facts on which the complaint is based;
- Contact details for sending a reply;
- Client signature (when a complaint is sent by post to the address of the Bank's head office).

A compensation claim must contain all the mandatory elements of a complaint and has to be submitted in writing. If it is not submitted in writing or is incomplete, the conditions for its consideration shall not be fulfilled.

The Bank shall only handle complete and properly submitted complaints. In the case of incomplete, incomprehensible or unclear complaint, the Bank shall invite the User to supplement the complaint within an 8-day deadline. The invitation for complaint supplementation shall interrupt the complaint-handling deadline. In this case, the complaint procedure, and thus the deadline for resolving the complaint and submitting the reply to the complaint, will begin on the day following the day of the receipt of a complete or supplemented complaint. If the User fails to supplement the complaint within the indicated deadline, the Bank will reject it.

The Bank will decide on the complaint as soon as possible or no later than 15 working days after the receipt of all relevant documentation. If it is not possible to resolve the complaint or objection within the indicated deadline due to the complexity of the case, the Bank shall inform the User in writing of the reasons thereof and the estimated date of the final solution of the complaint, which shall not exceed 35 working days from the date of receipt of the complete complaint. The User has the right to file an objection to a solution of the complaint. The Bank shall send a decision on the objection with appropriate explanations in writing to the client's address within 15 working days. This shall constitute the final decision of the Bank and the Bank's internal complaint procedure shall thus be completed.

(3) At any time, the User shall have the right to bring an action to resolve the dispute between him and the Bank at the court of competent jurisdiction.

(4) Local court of competent jurisdiction shall have jurisdiction to solve all prospective disputes, which may arise pursuant to these General Terms and Conditions and which the User and the Bank may not be able to solve consensually.

XV. Preliminary and final provisions

(1) In accordance with applicable law and/or its business policy, the Bank may modify and supplement these General Terms and Conditions. The Bank shall forward the body of modified General Terms and Conditions of its business operations to the User via electronic and/or mobile banking systems, it shall also publish it on its website and it shall be available in all its business units.

(2) If the User does not agree with modifications, which have been made to General Terms and Conditions, he may terminate his contract, which has been concluded on the basis of these General Terms and Conditions, with 15 days' notice. The User shall send his withdrawal from the contract to the Bank in writing no later than within 15 days of release of modified General Terms and Conditions. If the User does not notify the Bank about his disagreement with modifications within this time-limit, it shall be considered that he agrees with modifications. In case the User rejects suggested modifications in writing, but does not terminate his contract, it shall be considered that

the Bank has terminated the contract with 15 days' notice, which starts to run on the day a written termination has been sent.

(3) If the Bank does not receive a letter of termination, it shall be considered that the User has consent to modifications or supplements to these General Terms and Conditions.

(4) A component part of these General Terms and Conditions shall be the following documents:

a. Recommendations for Pursuit of Payment Transactions via Electronic Banking Systems for Legal Entities, Entrepreneurs and Individual Proprietors in UniCredit Banka Slovenija d.d.

b. Technical Requirements for electronic and/or mobile banking systems which are together with the General Terms and Conditions published on the website of the Bank: https://www.unicreditbank.si/si/podjetniki-in-mala-podjetja/digitalno-bancnistvo-za-podjetnike/e-bank.html#dokumentacijainobrazci.

(5) All instructions in relation to the use of electronic and/or mobile banking systems as well as to completion and implementation of payments shall be available to the User and the Authorized Person on the Bank's website and in electronic and/or mobile banking systems under the Help option.

(6) The Bank, the User and the Authorized Person shall agree to mutually recognize validity of electronic messages, which are envisaged in the package software of electronic and/or mobile banking systems, in Court.

(7) The User shall have the right to require a copy of General Terms and Conditions in paper form or other permanent data carrier at any time.

(8) The law of the Republic of Slovenia shall apply for provision of servicesin accordance with these General Terms and Conditions and for their interpretation.

(9) If the User detects that a breach making up the offence under the Payment Services, Services of Issuing Electronic Money and Payment Systems Act has occurred at provision of services on the basis of these General Terms and Conditions, he shall have the right to file a written proposal to initiate criminal proceedings. The proposal shall be filed with the Bank of Slovenia, which is competent for ruling on such offences.

(10) General Terms and Conditions are drawn up in the Slovenian language.

(11) These General Terms and Conditions shall apply as from 5th of October 2025.