GENERAL CONDITIONS FOR THE USE OF THE SYSTEM OF ONLINE AND MOBILE BANKING FOR CONSUMERS

I. Introductory Provisions

With the General Terms and Conditions for the Use of the Online and Mobile Banking System (hereinafter: General Terms and Conditions), UniCredit Banka Slovenija d.d. (hereinafter: the Bank) determines the obligations, rights, and conditions for the use of banking services through the online banking system Online Bank, the mobile banking system Mobile Bank GO! and Online Business web portal. The individual terms defined below have the following meanings:

(1) the **issuer** of the General Terms and Conditions is UniCredit Banka Slovenija d.d., Ameriška ulica 2, 1000 Ljubljana, Slovenia, swift code BACXSI22, info@unicreditgroup.si, www.unicreditbank.si, registered with the District Court in Ljubljana, application no. 1/10521/00, registration number 5446546. The Bank is on the list of banks and savings banks that hold the Bank of Slovenia authorisation to provide payment services, which can be found on the Bank of Slovenia website. The body responsible for the supervision of the issuer is the Bank of Slovenia;

(2) a **user** is a consumer who is a natural person and whose operations are enabled by the bank via the online and/or mobile banking systems for purposes outside his/her gainful or professional activity;

(3) a **legal representative of the user** is a natural person who represents the user in accordance with the law;

(4) an **authorised signatory** is a natural person who has the legal capacity and who is authorised by a user or a user's legal representative to use the online and/or mobile banking system by specifying the name of an authorised signatory on the banking form: Competences of the online and mobile banking system authorised signatory. In the event that the person authorised for work in online and /or mobile banking systems is allocated the competence of a signatory, the signature category shall be in accordance with the internal banking form "Authorization for disposing of funds in the current account";

(5) An **online bank** operates in a web browser and provides a user with banking services;

(6) **Mobile Bank GO! (**hereinafter referred to as Mobile Bank) is a mobile application that runs on mobile devices with Android, iOS or HarmonyOS operating systems and allows a user to perform certain banking services;

(7) the **closed system** represents operations between a user and the Bank with a special written agreement in accordance with paragraph 2 of the article 2 of Regulation (EU) no. 910 / EU. Closed systems in the Bank are: Online Bank, Mobile Bank and Online Business web portal. Electronic signatures in the closed system have the same legal effect as handwritten signatures;

(8) **personal security** elements are personalized features and other electronic signature creation devices provided to the user by the Bank for the purposes of authentication and electronic signing of payment orders, consents, contractual documentation and orders to the Bank. They differ according to the type of service and the type of closed system and are as follows: a physical token, a mobile token and personal PIN password;

(9) **third party providers** (TPP) are registered providers licensed by the Bank of Slovenia to provide new payment services, such as payment order (PIS – PAYMENT INITIATION SERVICE) and the provision of account information (AIS – ACCOUNT INFORMATION SERVICE). Third-party service providers can access a user's account only with their consent which is signed electronically by the user after a successful authentication using the Online Bank system or the Mobile Bank application.

The list of providers licensed to provide new payment services is published on the Bank of Slovenia website (https://bsi.si);

(10) **authentication** is the process that allows the Bank to verify the identity of a user or the justification of the use of a particular payment instrument, including the use of a user's personal security features;

(11) **strong customer authentication** is authentication using two or more elements that fall into the category of user knowledge (something that only a user knows), user ownership (something that is owned exclusively by a user), and inseparable connection with a user (something that the user is) which are independent of each other, which means that a breach of one element does not reduce the reliability of the others, and are designed to protect the confidentiality of the data being verified;

(12) a **physical token** is an electronic device that is protected by a 4-digit personal password and generates time-based one-time passwords that uniquely determine the authentication of a user or an authorised signatory in the online bank. The unique numeric password from a token, together with a username determined by the authorised signatory herself/himself, ensures unambiguous authentication of the authorised signatory when logging in and when signing with an electronic signature in the system of internet banking Online Bank, Mobile Bank and the Online Business web portal.. The use of a token is limited to one user only. Strong authentication in online banking requires a user to additionally generate a time-based one-time password for signing (OTP - One Time Password) with a physical token: by means of such an OTP, a user confirms the execution of the transaction or consent together with a summary of the transaction or consent to the Bank;

(13) a **mobile token** is software that represents an integral part of the Mobile Bank mobile device application or a standalone application, and it generates time-based one-time numeric passwords that unambiguously determine the authentication of a user or a proxy when entering or signing electronically in the internet banking system Online Bank, Mobile Bank and the Online Business web portal .;

(14) **personal PIN password** (hereinafter: PIN) is a secret personal authentication number selected by a user and consists of a sequence of numbers with which the user identifies himself when entering a mobile token. The PIN shall not contain fewer than 6 and no more than 8 digits. After entering an incorrect PIN three times, the software displays the incorrect security flag which informs a user that she/he has entered an incorrect personal password;

(15) **fingerprint** or **face ID** (Face ID on iOS) are biometric user identifiers and can be used instead of a personal password or PIN code to enter the Mobile Bank to confirm payment orders in Mobile Bank and to confirm online transactions with the help of Mobile Bank The module for authentication of fingerprints or for face recognition in your device is not provided by the Bank. Your fingerprint or face is stored on your mobile device, so you need to ensure their safe handling and proper storage and protection on your mobile device. The Bank does not process fingerprint and face image data (for example, does not store or access it), which means that the Bank is not the controller of such personal data. Additionally, such data cannot be processed by a contractual processor on behalf of the Bank. Taking into account the above, the Bank does not ensure compliance of the processing of such personal data with the Personal Data Protection Act (ZVOP-1) or the General Data Protection Regulation (GDPR). The Bank is not responsible for nor shall it guarantee the security of the fingerprint authentication and facial recognition function on any device, and the Bank is also not responsible for the operation of the function in the manner presented by the device manufacturer;

(16) the **activation code** is a unique, time-based code sent by the system and is linked to the user of the Mobile Bank application and mobile token. After a successful activation, the activation code shall no longer be usable. The activation code is also no longer usable if a user does not activate the application within 72 hours of receiving the activation code for mobile bank GO! or mobile token;

(17) a **one-time numeric password** is used to authenticate synchronisation between a token and the backup system and is generated after entering the personal PIN code in the token. The PIN

consists of 6 digits and is valid for a limited period of time. Such a password can only be used once. It is possible to attempt to login unsuccessfully three times; after three unsuccessful login attempts, the intervention of a system administrator is required;

(18) the **username** is a unique set of alphanumeric characters with which the user or an authorised signatory identifies herself/himself when entering Mobile Bank GO!, Online Bank and Online Business web portal. Different users or authorised signatories cannot have the same username;

(19) the **security question** and its answer are the basis for the identification of a user, and they are both set by the user when opening a bank account online;

(20) an **electronic signature** is a set of data in electronic form, added to or logically linked to other data in electronic form and which the signatory uses to sign. An electronic signature replaces a handwritten signature and has the same probative value as a handwritten signature;

(21) **advanced electronic signature** is an electronic signature that is uniquely associated with a signatory, identifies a signatory, is created on the basis of electronic signature creation data that a high-confident signatory can use only under its control, and it is linked to the data signed in such a way that any subsequent change in the data is noticeable.

(22) a **signatory** is a natural person who creates an electronic signature;

(23) **electronic signature certificate** means an electronic certificate which connects the data for the validation of an electronic signature with a natural person and confirms at least the name or pseudonym of that person;

(24) **electronic signature generator** means a configured software or hardware used to generate an electronic signature.

(25) the **Bank's website** is the website http://www.unicreditbank.si and all its subpages;

(26) the **daily limit** is the maximum allowable amount of the sum of outflow transactions in one day;

(27) the **transaction limit** is the maximum allowable amount of an individual outflow transaction;

(28) **durable medium** means any instrument which enables the user to store information addressed personally to him in a way accessible for future reference for a period of time adequate to the purposes of the information and which allows the unchanged reproduction of the information stored (e.g. paper-based notice, electronic notification form in PDF format);

(29) **payment instrument** is any device or set of procedures or both agreed upon between an individual user and the Bank which is bound only to that user and which can be used by the user in order to initiate a payment order;

(30) **e-invoice** is an invoice issued in a standard electronic form and serves as an equivalent replacement for a paper invoice, which is forwarded by an issuer to the invoice recipient paying for the service/goods etc. provided. The e-invoice complies with the legal regulations governing this area;

(31) the **e-invoicing exchange system** renders possible a smooth and successful exchange of e-invoices for all participants: issuers, recipients, intermediaries, and archivists;

(32) **e-application** is an electronic form of application for receiving an e-invoice and is performed by a user via the Online Bank. An e-application is forwarded via the system to the issuer of the e-invoice specified in the e-application. A user performs an e-login for each e-invoice issuer separately;

(33) **e-unsubscription** is an electronic form of unsubscribing from receiving an e-invoice and is performed by a user via the Online bank. The e-unsubscription is forwarded via the system to the issuer of the e-invoice specified in the e-unsubscription. The user performs e-unsubscription for each e-invoice issuer separately;

(34) a **recipient of the e-invoice** is a natural person who has opened a transaction account with the Bank and is a user of the Online Bank, having a business relationship with the issuer of the e-invoice;

(35) **e-invoice issuer** is a legal entity that has officially established a business relationship with the recipient of an e-invoice on the basis of which it issues an e-invoice to the recipient; the online and mobile banking accession statement for the use of the online and/or mobile banking system for natural persons is filled out by a user who wants to activate, change or block the online and/or mobile banking system. She/he submits it in the Bank branch managing her/his personal bank account;

(36) an **order** represents a request for the performance of banking services which the user sends to the Bank using the Online Bank, Mobile Bank systems or Online Business web portal after a successful authentication and electronic signature.

II. Protection of Personal Data and Confidential Information

(1) The Bank shall be the controller of personal and other confidential information on the user which the Bank obtains upon the establishment of a business relationship and during further business with the user.

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

(3) In the online and mobile banking system, the Bank processes, inter alia, the following personal data: sociodemographic data (e.g. gender, age, status, marital status, education, employment data), geolocation data, contact data (e.g. telephone number, e-mail address, residential address), data on personal documents submitted by the individual to the Bank, and other business data of the individual, in particular transaction data (whereby transactions in online and mobile banking are also categorized), data on channels and applications through which an individual contacts the Bank, information on the IP address (e.g. when accessing the Online Bank environment), and information on the individual's use of services and products.

(4) Pursuant to the provisions of Articles 13 and 22 of the General Data Protection Regulation, we inform you that the Bank uses automated decision-making for the purposes of fraud prevention, whereby the bank will process the transactional data of transactions made using internet and mobile banking applications. Such processing is necessary on the basis of applicable legislation as specified in article 22(2)(a). No special types of personal data are processed. If you do not agree with the result of the automated decision of the payment fraud prevention system, you can challenge this decision by stating your position and requesting the Bank to have the decision reviewed by a Bank employee.

(5) 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. The currently valid General Information on Personal Data Processing is available at the Bank's business premises and on its website (www.unicreditbank.si/gdpr).

(6) The user (and also any potential guarantor and/or pledger) undertakes to notify the Bank of any change in place of residence or employment, and any major changes in their financial position and income no later than 8 days after the change has occurred. At the same time, the user (and also any potential guarantor and/or pledger) allows and authorises the Bank or any other person who acquires, through cession, the rights stemming from the contract or business relationship with the Bank to make inquiries with the competent authorities about the place of residence, employment, and financial

situation, including inquiries regarding the existence and status of transaction accounts opened with banks.

(7) The user agrees that the Bank periodically verifies user data in order to determine – for the requirements of the FATCA (Foreign Accounts Tax Compliance Act) – whether any circumstances have occurred (U.S. Indicia) that could cause a user to be considered a US taxable person (U.S. Person). Notwithstanding the above provision, the user undertakes to immediately notify the Bank, in writing, of any change in the circumstances of their status (U.S. Indicia), such as the acquisition of the following: US citizenship, a residence address in the USA, a phone number in the USA, etc. The user undertakes to communicate and forward to the Bank the relevant documentation demonstrating any change in circumstances.

(8) If the user fails to communicate and provide the Bank with all relevant documents immediately upon the receipt of a written request from the Bank/UCB asking the user to provide the relevant documentation showing the status of the user, the Bank will notify the tax authority of the Republic of Slovenia that the user is a potential US taxable person (U.S. Person). In this case, the Bank shall be entitled to unilaterally terminate the contractual relationship, after a prior written notification to the user, and to close the account in accordance with the provisions of the General Terms and Conditions.

(9) The user undertakes to refund the Bank for any costs and damage that may incur as a result of the user's violation of this article.

(10) The Bank and the user agree that by signing the agreement in accordance with paragraph 2 of Article 215 of the Banking Act, the user agrees that the bank may communicate individual confidential data on the user to the tax authority of the Republic of Slovenia for the needs of the FATCA.

III. The Main Features of the Online and Mobile Banking Systems

(1) A user, an authorised signatory, and the Bank agree that the online banking system shall use a token or a mobile token along with the corresponding PIN code for authentication and that the mobile banking system shall use a mobile token along with the corresponding personal PIN for authentication.

(2) Online banking enables a full provision of payment services at home and abroad. It provides a high level of security by using a PIN code or a fingerprint, a time-based password, a public certificate for encrypting the transferred data, and a username. The online banking system can provide a user or an authorised signatory with the following online services:

- provision of payment services,
- monitoring the bookkeeping and current balance in the accounts,
- exchange of messages between a user or an authorised signatory and the Bank,
- changing the daily and transaction limits set by the Bank when opening an account, therefore a user can change the value of the limits at her/his own will,
- changing security settings (security question and answer),
- setting of notifications of inflows and outflows received via e-mail, and
- other online services described in the Online Banking Instructions.

Online banking can also be used on mobile and other devices (GSM phones, smartphones, PDAs, tablets, etc., hereinafter referred to as mobile devices) whose operating system and browser provide access to the internet.

The Bank enables the use of Mobile Bank on only one device.

(3) Mobile Bank provides an insight into banking services and allows a user to perform certain banking services in the Online Bank system using software that the user downloads to his mobile device from the Apple Store, Google Play and Huawei AppGallery online stores or via a hyperlink received in an SMS message. The user activates the application or software with an activation key, which is also received via SMS. To use mobile banking, the mobile device on which the application is installed must allow an internet connection. Access to financial data and functionality of the mobile banking shall not be rendered possible without a personal PIN password which is known only to the user.

(4) Upon accessing the mobile bank and until revoked, the existing user authorisations apply to all accounts on which the user is authorised in the Online Bank system, or they shall be reduced in accordance with the restrictions and characteristics of the mobile bank. The characteristics and limitations of the mobile bank are published on the Bank's website http://www.unicreditbank.si/GO and may be subject to change.

Mobile bank may provide the following services to a user or an authorised signatory:

- insight into the balance and turnover on holder and authorised transaction, savings, and deposit accounts,
- transactions and payment card details,
- payments by universal payment orders and internal transfer of funds between the same user's accounts with the Bank,
- exchange rate and currency conversion tool,
- access to documents (bank statements, certificates), and
- other online services described in product presentations for each customer segment.

(5) The valid daily limit in the mobile bank is determined by the Bank and published on the Bank's website https://www.unicreditbank.si/GO. In the event of selecting a lower transaction or daily limit in the Online Bank system, the lower limit is taken into account in the mobile bank.

(6) Online Business web portal is a web portal of UniCredit Bank, which enables e-commerce at a distance to existing users of Online Bank or Mobile Bank. Through Online Business web portal client can order various banking products, electronically sign contracts and other banking documents with a valid advanced electronic signature within the closed system and without need of visiting a branch.

IV. Manner and Means of Communication

(1) In order to use the online and/or mobile banking system, a user or an authorised signatory must possess the appropriate computer (hardware and software) or the appropriate mobile device and communication equipment as specified in the Technical Requirements. The valid Technical Requirements for the system are published on the Bank's website www.unicreditbank.si and they represent mandatory instructions for users regarding the manner and appropriateness of the use of online and mobile banking as well as other important instructions for the use of online and mobile banking.

(2) The Online Bank,Mobile bank and Online Business web portal is a closed system in accordance with paragraph 2 of the article 2 of Regulation (EU) no. 910 / EU. All electronic notifications and documentation provided by the Bank to a client or an authorised signatory via Online Bank Mobile bank and Online Business web portal are equivalent to paper statements sent by the Bank by post.

(3) Mobile banking enables a user and an authorized signatory to review the sent orders which are available to the user under an individual account in the mobile bank.

(4) Based on the user's order placed through the online banking system or in the Bank branch, the Bank forwards to the user all transactions performed via the mobile bank on paper or another durable medium.

(5) The user can set up an automatic notification via e-mail about the balance of accounts and outflows and inflows within the Online Bank in accordance with the Instructions for the use of the Online Bank.

(6) The user or the authorised representative of the Online Bank receives from the Bank all notifications, monthly statements, electronically signed documents, contractual documentation, and other documents (hereinafter: electronic notifications and documentation) in electronic form. The received electronic notifications and

documentation can be found in the Online Bank in the menu Overview of Statements and Contracts. The Bank sends electronic notifications and documentation in paper form to the user or authorised person only upon her/his prior explicit request in the form of an order placed through the online banking system or in the Bank's business unit. In the event that a user or an authorised signatory no longer wishes to use the online banking, she/he is obliged to transfer and save electronic notifications and documentation on the permanent data carrier located in the menu Overview of Statements and Contracts before closing the Online Bank so that these documents shall be available to him in electronic form for later use.

V. Acquisition of an Online and/or Mobile Banking System

(1) The Bank approves the use of online and/or mobile banking by the user if she/he:
- provides the Bank with all duly completed original bank forms,
- has a transaction account opened with the Bank,
- operates a transaction account in accordance with the general conditions, and regularly settles all his/her liabilities.

(2) The Bank reserves the right to not approve the use of the online and/or mobile banking system without stating the reasons for the refusal. It shall notify a user and, if necessary, an authorised signatory in writing about its decision.

(3) One or more authorised signatories can be authorised by the user or the user's legal representative. The type of authorisation for an individual authorised signatory is determined by the user or her/his legal representative by means of the appropriate bank form. Upon receiving a correctly completed bank form, the Bank activates the authorised signatory authorisation.

(4) The user can order the Bank to change the authorisation of an individual authorised signatory on the appropriate bank form.

(5) In the event that an authorised signatory is assigned the authority of online signing, the data about the authorised signatory must be in accordance with the data specified in the bank form "Authorisation To Dispose of Funds in the Current Account" of the user.

(6) The Bank can approve the user of the Online Bank system to order and use the Mobile Bank on the basis of a user's order made through the Online Bank or upon filling out an application for the use of the online and/or mobile banking system, which shall afterwards be submitted at any of the Bank branches.

(7) Ordering and activating the service is a prerequisite for using the service.

(8) The contract is considered concluded on the day when the Bank approves the use of the services of the Online bank system and/or the Mobile Bank application.

(9) By signing the application or contract, the user confirms that she/he accepts the applicable general terms and conditions.

VI. Acquisition of Funds Authentication and Devices for Electronic Signing

(1) To access the Online Bank system, a user can choose to use only one of the possible means of authentication, either a token or a mobile token, and the choice shall be determined by the user, who orders the selected option at the bank. Upon receipt of a token or a mobile token, a user or an authorised signatory assumes full responsibility for the storage of the selected token and for actions resulting from the use of online banking. The selected token is owned by the Bank and it is leased to the user or authorised signatory for the period of use of the Online Bank system.

(2) In the event of ordering and concluding a contract for the Mobile Bank service, a user or an authorised signatory who is authorised to use this application also receives a mobile token as a stand alone application upon receiving the application. After a successful activation with the prior use of a personal PIN password, the mobile token generates a one-time and time-based password for entering or confirming the online bank which unambiguously determines the authentication of the user or authorised signatory.

(3) The username, which is determined by the user or the authorised signatory herself/himself, along with the numerical personal password PIN or a fingerprint and a unique password generated by the token on the basis of a personal PIN password, ensure unambiguous authentication of the user or authorised signatory when logging in to the Online Bank, Mobile Bank and Online Business web portal and when confirming individual actions (payments, bank orders, signing documents).

(4) On the document, which is electronically signed by the user or the authorized person with the electronic signature creation device, visual interpretation of the electronic signature contains at least the name and surname of the signatory and the date and time of the electronic signature.

(5) Electronic signatures created within a closed system of the Bank have the same validity and probative value as a handwritten signature. And therefore all documents signed with any type of electronic signature created in a closed system of the Bank are considered to be handwritten.

VII. Execution of Payment Orders

(1) The Bank is considered to have received a payment order when a user or an authorised signatory (in accordance with the signature rights on the account) signs and sends the order via the online and/or mobile banking system to the bank server. The Bank provides information on the status of individual payment orders to the user or the authorised person with feedback via the online and/or mobile banking system.

(2) The Bank shall provide a user and an authorised person with the execution of all correctly completed payment orders within the deadlines prescribed or agreed for an individual type of payment order, in accordance with the Schedule of Operations With Transaction Accounts (hereinafter: Schedule). If a user or an authorised signatory decides to cancel a payment order, this can be done via the online or mobile banking system, in accordance with the deadlines specified in the Schedule.

VIII. E-invoices in the Online Bank System

(1) The Bank enables users of the Online Bank system to register for/unsubscribe from e-invoicing as well as to receive and execute e-invoices in the form of payments in the online bank.

(2) The Bank of the e-invoice recipient is obliged to:
a. receive e-invoices that have arrived in the e-invoice exchange system,
b. make the e-invoices that have been received available to the user within the Online Bank system,
c. send feedback on the delivery of the e-invoice to the recipient.

(3) The user of the Online Bank system logs in to receive the e-invoice. The Bank forwards the e-application via the e-invoice exchange system to the e-invoice issuer for whom the e-application was intended. The Bank does not guarantee that the issuer of the e-invoice will accept the e-application and start issuing the e-invoice to the user. The issuer of the e-invoice forwards the e-invoice through its bank to the bank of the e-invoice recipient, and the latter forwards it to the Online Bank. The recipient of the e-invoice can e-unsubscribe via the Online Bank system, thus unsubscribing from receiving the issuer's e-invoices.

(4) The user can sign up to receive e-invoices from issuers that are included in the e-invoice exchange system.

(5) The user shall resolve any issues arising from the content of the received e-invoice (incorrect data, inappropriate content, incorrect invoice) directly with the issuer of the e-invoice. Complaints arising from the operation of the e-invoice system within the Online Bank system shall be resolved by the Bank.

IX. Blockage or Termination of the Use of Online and/or Mobile Banking System

(1) A user or an authorised signatory may, with the consent of the Bank, cancel the use of the online and/or mobile banking system without notice. A user or an authorised signatory may cancel the use of the online and/or mobile banking system with a one-month notice period. The proposal to terminate the use of the online and/or mobile banking system must be submitted to the Bank on the appropriate bank form.

(2) The Bank may, at its own discretion, terminate the use of the online and/or mobile banking systems with a two-month notice period.

(3) The Bank reserves the right to restrict or terminate access to the online and/or mobile banking systems for a certain period of time without prior notice, especially if critical events (primarily those related to security) have occurred, if these general conditions are not met, in case of incorrect business operations of the user or if there is the suspicion or possibility of abuse.

(4) On the day of termination, the Bank blocks the use of online and mobile banking and settles all outstanding obligations of a user or an authorised signatory in accordance with the Decision on the Tariff of Payments for Retail, Small Businesses, Sole Proprietors and Freelancers (hereinafter: the Tariff).

(5) All orders sent to the online bank prior to the cessation of use will be executed according to the Schedule, provided that all the necessary conditions are met.

(6) At the user's request, the Bank may block a valid means of authentication for the accounts for their authorised signatories on the basis of the completed form Competencies of the System Authorised Signatory.

(7) The Bank can block and/or terminate a user or an authorised signatory on the basis of the completed banking form Application for activation, change or blocking of the online and mobile banking. A user's or an authorised signatory's competencies specific to her/his bank accounts indicated on the form are blocked and/or revoked.

(8) The Bank will block the service immediately upon receipt of notification of theft/loss/misuse and upon receipt of all data necessary to impose a blockade and inform the user thereof.

(9) All documents must be submitted in their original form and shall be signed by the user or the user's legal representative and her/his banking advisor.

(10) The request for blocking can be submitted by the user, their authorised signatory, or their legal representative:

in person, during working hours, at the Bank's branch managing their personal account. The information on working hours is published on the Bank's website www.unicreditbank.si;

- via the contact center on 01 5876 600.

(11) The person revoking is responsible for the veracity of the information provided. Upon receipt of the notification, the Bank shall disable the possibility of sending payment orders via online and/or mobile banking systems or block or withdraw the authorisation of an individual user or authorised person to use the online or mobile banking system.

X. Obligations of the User and the Authorised Signatory

(1) The user and the authorised signatory undertake to:

- protect the software and use it only for the procedures intended for the use of online and mobile banking system;
- secure carefully and in a manner that will prevent damage or misappropriation the following items: the token, mobile token, username, password, PIN code and, in the case of the use of the mobile banking service, the personal PIN password;
- carefully store means of authentication, usernames, and passwords, and protect them by preventing loss, theft, or misuse;
- not write down passwords and usernames on paper, online, or other media;
- change their personal identification number (PIN) at least once a month;
- regularly update the application and review data;
- regularly review notifications sent by the Bank;
- comply with the instructions for the use of the online and mobile banking systems and the applicable legislation;
- immediately notify the Bank of any detected irregularities or atypical operation of the online or mobile banking system;
- immediately notify the Bank of any unauthorised use or suspicion of unauthorised use of the online or mobile banking system and submit to the Bank a written request for a blockade; and
- notify the Bank of any abuse or suspected misuse of the online and mobile banking system and submit to the Bank a written request for a blockade.

(2) The user undertakes to:

- immediately notify the Bank of changes to or termination of the powers of an individual authorised signatory; and
- keep records of its authorised signatories and their competencies.

XI. Bank's Responsibility

(1) Upon accession to the use of the online or mobile banking system, the Bank shall provide the user and the authorised signatory with all the elements necessary for the use of the online or mobile banking system.

(2) The Bank shall ensure that the user and the authorised signatory have the uninterrupted use of the online or mobile banking system. Exceptions are related to outages due to cases of force majeure, technical problems, other unexpected outages, and in the event of announced system outages.

(3) The Bank shall not be liable for any damage resulting from extraordinary circumstances and events, such as but not limited to: cases of force majeure, strikes, decisions and actions of public authorities, disruptions in telecommunications and other traffic, errors in the transmission of data over telecommunications networks, denied access to online or mobile banking systems.

(4) The Bank shall not be liable for any damage that may occur to the user or authorised signatory due to the failure of online or mobile banking systems, telecommunications, or computer systems and/or mobile devices which could occur due to unjustified interventions of the user or third parties.

(5) The Bank shall be held liable to the user or authorised signatory for any material damage that may have occurred intentionally or through gross negligence on the part of the Bank. The Bank shall only be held liable for direct damage. In the event of the discovery of errors, irregularities, or in the event of damage, the user or authorised signatory shall act with all due diligence and in accordance with these General Terms and Conditions.

(6) The Bank shall not be held liable in the event of the loss or destruction of data and equipment of the user or authorised signatory due to the installation and use of the online or mobile banking system.

(7) The Bank shall not be held liable for any damage in cases where the user does not keep her/his own records of authorised signatories, their payment instruments - devices for creating electronic signatures, or their powers with regard to the user's accounts.

XII. Fees

(1) The Bank shall charge the user and authorized signatory the cost of maintaining online and mobile banking services in the amount specified in the currently valid Bank Tariff, which is published on www.unicreditbank.si. The user expressly agrees that the Bank shall directly debit the user's account for the cost of maintaining the online and mobile banking services and other related costs.

(2) When activating the online and/or mobile banking services by the 15th of the month, the cost of a one-time entrance fee and maintenance of the online and mobile banking services will be

charged in the current month by directly debiting the user's transaction account. In cases in which the service is activated after the 15th of the month, the costs shall be charged in the following calendar month.

(3) In the event of destruction, misappropriation, or loss of an asset for authentication, all costs of creating a new asset shall be paid by the user or authorised signatory.

(4) We would like to point out that in the event of three consecutive incorrect entries of the personal password PIN in the mobile banking application, the application will be locked automatically. After the Mobile Bank is reactivated, the Bank re-enables the user to perform tasks related to banking operations and charges the user in the amount specified in the currently valid Tariff of the Bank.

XIII. Amicable Dispute Resolution

(1) Any disputes, disagreements or complaints regarding the provision of services in accordance with these General Terms and Conditions will be resolved amicably by the user or authorised signatory and the Bank.

(2) Any disputes and disagreements shall be resolved by the Bank on the basis of a written or oral complaint submitted by the user and/or cardholder (hereinafter: the complainant). The complainant may address a written complaint to the Bank using a prescribed form available at all Bank branches and send it to UniCredit Banka Slovenija d.d. Ameriška ulica 2, 1000 Ljubljana (with the note: Monitoring of complaints), via the Online Bank electronic banking system, by e-mail to the competent contact person at the Bank branch, to the general e-mail address of the Bank info@unicreditgroup.si, or via the web portal https://www.unicreditbank.si/si/o-nas/pripomocki/pritozbeni-postopek.html . The complainant may file an oral complaint in person or by telephone at all business units of the Bank or by telephone 01 5876 600 to the Bank's contact centre. The Bank shall respond in writing only to complaints submitted in writing. The client's complaint shall be comprehensible and clear and shall contain the facts on which the complaint is based. The complaint shall contain the information on the client filing the complaint (name, surname, address, e-mail address, telephone); explanation of the reasons to complain, description of the event or indication of key facts and date of the event; indication of the documents to which the complaint relates; submission of evidence to confirm the facts on which the client's claim is based; contact details for sending the answer; signature of the client (in case of submitting a complaint by post to the address of the Bank's registered office). The party's claim for damages shall be submitted in writing and shall contain all the mandatory elements of the complaint. If it is not submitted in writing or is not complete, the conditions for dealing with it are not met. The Bank shall only handle complaints that are complete and submitted correctly. If the client's complaint is incomplete, incomprehensible or unclear, the Bank shall invite the client to complete the complaint and shall set an 8-day time limit for completing it. The request to supplement the complaint suspends the complaint-handling time-limit. In this case, the complaint procedure, and thus the time limit for resolving the complaint and sending the response to the complaint, shall begin to run on the day following the day of receipt of the complete or supplemented complaint. If the client fails to supplement the complaint within the time-limit prescribed, the Bank shall reject it. The competent body at the Bank shall decide on the complainant's claim within the shortest possible time or at the latest within the time limit determined for individual types of complaints by the applicable regulations. The Bank shall send a reply to the complainant's claim with appropriate explanations in writing to the complainant's address. The Bank shall reply to complaints regarding the performance of payment transactions which are covered by the provisions of the Payment Services, Electronic Money Issuance Services and Payment Systems Act (ZplaSSIED) within 15 business days following the receipt of all relevant documentation. If due to exceptional circumstances the reply is not possible within 15 business days, the Bank shall send a temporary answer to the client in which it explains the delays or gives an appropriate explanation to the client and sets a deadline by which the client will receive the final answer. This period may not exceed 35 business days. In case of complaints that do not relate to payment transactions, the Bank shall provide a reply to the client within 8 days of receipt of all relevant documentation. The complainant shall have the right to file an objection to the Bank's reply. The Bank shall send the decision regarding the objection with adequate explanations in written format to the claimant's address within 15 business days. By doing so, the Bank's decision shall be final and its internal complaint procedure shall be concluded.

(3) If the complexity of the case does not allow the resolution of the claim or objection within the specified period, the Bank shall notify the complainant in writing of the anticipated date of the resolution of the complainant's claim or objection.

(4) If the user does not agree with the decision on her/his complaint or if she/he does not receive a response from the Bank regarding the complaint within 30 days, the user has the right to file, no later than 13 months after the final decision in the internal complaint procedure is established, an initiative for an out-of-court settlement procedure with the non-judicial dispute resolution provider (hereinafter: NJDR Provider), which the Bank recognises as competent for resolving consumer disputes. The Bank may at any time change the non-judicial dispute resolution provider competent for the settlement of consumer disputes.

(5) The name, electronic address, and phone number of the acknowledged NJDR provider shall be published on the Bank's web page www.unicreditbank.si.

(6) The filing of an initiative does not interfere with the user's right to file an appropriate request for resolving a dispute with the locally competent court according the seat of the Bank.

XIV. Transitional and Final Provisions

(1) If the Bank makes amendments to these General Terms and Conditions, it shall inform the user via the online or mobile banking systems two months before the amendments enter into force by sending her/him a proposal regarding the amendment of the General Terms and Conditions.

(2) If a user does not agree with the amendments to the General Terms and Conditions, she/he may withdraw from the use of online or mobile banking systems without notice or payment of fees. The request shall be submitted by the user in writing no later than the day before the specified day when the amendment is to enter into force. If the user fails to notify the bank of their disagreement with the amendments within this period, it shall be understood that they agree with the amendments. If a user rejects the proposed amendments but does not terminate the agreement regarding the use of online and mobile banking, it shall be understood that the Bank terminated the agreement with a two-month period of notice, counted from the day when the notification of the amendment is sent.

(3) The currently valid General Terms and Conditions shall be published on the Bank's website and in all Bank branches.

(4) The document Technical Requirements for Electronic Banking Systems is an integral part of these General Terms and Conditions.

(5) All instructions regarding the use of online or mobile banking systems, filling out forms and making payments are available to the user and the authorised signatory on the Bank's website and in the online banking system under the Help option.

(6) The Bank, the user and the authorised signatory agree to mutually recognise the validity of electronic messages and electronic signatures in court within closed online or mobile banking systems.

(7) The user has the right to request, at any time, a copy of the General Terms and Conditions on paper or another durable medium.

(8) Services carried out under these General Terms and Conditions and the interpretation of these Terms and Conditions shall be governed by the law of the Republic of Slovenia.

(9) If the user becomes aware of a breach committed in carrying out services under these General Terms and Conditions, and such a breach constitutes an infringement under the ZPlaSSIED, they shall have the right to file a written proposal to initiate misdemeanour proceedings. The proposal shall be lodged with the Bank of Slovenia which is responsible for deciding on such offenses.

(10) The General Terms and Conditions are drawn up in Slovene.

(11) These General Terms and Conditions shall apply as of 29 of June 2024.