GENERAL TERMS AND CONDITIONS FOR THE USE OF THE ONLINE AND MOBILE BANKING SYSTEM BY RETAIL CLIENTS

I. Introductory Provisions

By way of these General Terms and Conditions for the Use of the Online and Mobile Banking System by Retail Clients (hereinafter: General Terms and Conditions), UniCredit Banka Slovenija d.d. (hereinafter: the Bank) lays down the obligations, rights and conditions for using and transacting via the Online B@nk online banking system. Individual terms defined below shall have the following meaning:

(1) **Issuer** of the General Terms and Conditions is UniCredit Banka Slovenija d.d., Šmartinska 140, 1000 Ljubljana, Slovenia, Swift code BACXSI22, info@unicreditgroup.si, registered with the District Court of Ljubljana, reg. No. 1/10521/00, reg. ID No. 5446546. The Bank is listed on the list of banks and savings banks that have been granted a permit by the Bank of Slovenia for the provision of payment services and is published on the web page of the Bank of Slovenia;

(2) **User** shall be a retail client who is a natural person and whom the Bank has enabled to transact via the online and/or mobile banking system for the purposes that are not the purposes of their gainful or professional activity;

(3) **User's Legal Representative** shall be a natural person who represents the User in accordance with the law;

(4) **Person Authorised for Use** (hereinafter: Authorised Person) shall be a natural person with the capacity to contract and whom the User or the User's Legal Representative authorises for the use of the online and/or mobile banking system by indicating them on the bank form entitled Authorisations of the Authorised Person for the Online and/or Mobile Banking System. If the Authorised Person is granted the authority to sign payment orders in the online and/or mobile banking systems, the category of the signature must correspond with the internal bank form entitled"Authorisation to Dispose of the Funds on the Transaction Account";

(5) **Identification and Authentication Elements** shall be means that ensure the authentication (recognition/identification) of the User or Authorised Person for the use and issue of consent for the signing of payment orders. Identification and Authentication Elements may differ depending on the use of the services of either online or mobile banking and include the Token, M-Token, SMS-Token, PIN code, personal PIN password and other means for identification and authentication;

(6) **Token** shall be an electronic device that generates limited-duration one-time passwords that uniquely authenticate (recognise/identify) the User or Authorised Person in the Online B@nk system;

(7) **M-Token** shall be software that forms an integral part of the GO! Mobile Bank for mobile devices or an independent application for mobile devices that generates limited-duration one-time passwords that uniquely authenticate (recognise/identify) the User or Authorised Person in the Online B@nk system;

(8) **SMS-Token** allows unique authentication (recognition/identification) of the User or Authorised Person in the Online B@nk system. The User receives a one-time limited-duration password in the form of an SMS on their mobile phone number that they provided in the agreement on the activation of the SMS-Token service. The entry of a one-time limited-duration password allows the authentication (recognition/-identification) of the User or Authorised Person in the Online B@nk system and is used for the submission of orders, confirmation of data and signing of payment orders in the Online B@nk system.

(9) **PIN code** or personal identification number shall be a sequence of characters that are used together with the Token or M-Token to generate a numeric password that allows the authentication (recognition/identification) of the User or Authorised Person upon entry to the Online B@nk system, confirmation of data and signing of payment orders in the Online B@nk system;

(10) **Personal PIN Password** (hereinafter: the PIN) shall be a personal identification number comprising a sequence of digits used by the User orAuthorised Person to identify themselves upon the entry to the GO! Mobile Bank application or the entry to the M-Token service. Only the User knows their Personal PIN Password as they assign it themselves upon the first setup of the service, whereby the Personal PIN Password may not comprise less than 6 and more than 8 digits;

(11) **Activation Key** shall be a personal identification number used for the activation of the GO! Mobile Bank service, whereby the Activation Key is rendered unusable for any other purpose after the successful activation. The Activation Key is also rendered unusable if the User fails to activate the application within 72 hours of receiving the key;

(12) **Password** shall be a sequence of digits generated by the Token, M-Token or SMS-Token and serves for the authentication of the User or Authorised Person;

(13) **Username** shall be a unique set of alphanumeric characters used by the User or Authorised Person to identify themselves upon the entry to the GO! Mobile Bank application Different Users or Authorised Persons cannot have the same Username;

(14) **Debiting Account** shall be the account that is indicated in the payment order, which is sent for execution, as the account number to be debited;

(15) **Business Day**: if the recipient holds an account with a bank that has its registered office in the territory of the Republic of Slovenia, a Business Day shall be any day with the exception of Saturdays, Sundays and work-free days according to the legislation applicable at any relevant time. If the recipient holds an account with a payment services provider that has its registered office outside the territory of the Republic of Slovenia, a Business Day shall be any day that is a Business Day in the Republic of Slovenia and simultaneously a Business Day of all participants involved in the execution of an individual payment transaction;

(16) **Durable Medium** shall be any instrument enabling the User to save data addressed to them personally so that they are later available for use for as long as necessary to achieve the purposes of such data, and which enables unmodified viewing of saved data (e.g. notice in paper form or notice in the electronic PDF format);

(17) **Payment Instrument** shall mean any device or set of procedures or both that are agreed between an individual User and the Bank. Such an instrument is associated exclusively with a particular User who can use it to submit a payment order;

(18) **E-Invoice shall be an invoice** issued in standard electronic format that is equal to and replaces an invoice in paper form, which is issued by the invoice issuer directly to the invoice recipient for the service rendered/goods delivered, etc. E-Invoice complies with the statutory provisions governing this field;

(19) **E-Invoice Exchange System** allows uninterrupted and successful exchange of E-Invoices to all participants: issuers, recipients, intermediaries and archivists;

(20) **E-Registration** shall be an electronic form of application for the reception of the E-Invoice submitted by the User via the Online B@nk e-bank. E-Registration is sent via the system to the E-Invoice issuer indicated in the E-Registration.The User submits an E-Registration for each E-Invoice issuer separately;

(21) **E-Deregistration** shall be an electronic form for deregistration from the reception of the E-Invoice submitted by the User via the Online B@nk e-bank. E-Deregistration is sent via the system to the E-Invoice issuer indicated in the E-Deregistration. The User submits an E-Deregistration for each E-Invoice issuer separately;

(22) **E-Invoice Recipient** shall be a legal entity or natural person holding a transaction account at the Bank and is a User of the Online B@nk, whereby they also have a business relationship with the E-Invoice issuer;

(23) **E-Invoice Issuer** shall be a legal entity that has a business relationship concluded with the E-Invoice Recipient, based on which it issues an

E-Invoice to the Recipient; the Registration Statement for Online and Mobile Banking for the Use of the Online and/or Mobile Banking System for Natural Persons is filled in by the User requesting the activation, modification or blocking of the online and/or mobile banking system. They submit it at the Bank's business unit that manages their personal account;

(24) **Order** shall be a request for the provision of a banking service that a User sends to the Bank following successful identification or authorisation by using the Online B@nk system or the GO! Mobile Bank application.

II. Protection of Personal Data and Confidential Information

(1) The Bank shall protect as confidential data all of the data, facts and circumstances on an individual User that it has at its disposal. The Bank shall protect all of the personal data of an individual User in accordance with the applicable legislation governing personal data protection. The Bank shall communicate said data only to the User, third parties for the purpose of fulfilling its obligations arising from the execution of the User's payment orders, and to competent authorities in accordance with the law, i.e. at their written request.

(2) The User and the Authorised Person agree with all of the data acquired being used, saved and included in databases as well as for them to be processed electronically using computers for the purposes of the Bank and the fulfilment of legislative and contractual obligations. The Bank may communicate the data to third party users, i.e. parent or sister companies within the UniCredit Group, for the purpose of complying with statutory provisions, the unification and optimum provision of banking and other financial services as well as for the purpose of other mutual contractual relations, which means the exporting of said data outside the Republic of Slovenia when the registered office of the parent or sister company is located outside the Republic of Slovenia.

III. Main Characteristics of the Online and/or Mobile Banking Systems

(1) The User, Authorised Person and the Bank agree that the Token, M-Token or SMS Token together with the associated PIN code being used in the online banking system for the purpose of identification and authentication and for the M-Token together with the associated Personal PIN Password being used for the purpose of identification and authentication in the mobile banking system.

(2) Online B@nk is an online banking system that is a product of the UniCredit Group. The program allows comprehensive execution of payment services at home and abroad. It provides a high level of security with the use of a PIN Code, limited-duration password, public certificate for the encoding of transferred data and the Username. The online banking system can provide the following services to the User or Authorised Person:

- provision of payment services;
- monitoring of the current and available balance on the accounts;
- exchange of messages between the User or Authorised Person and the Bank;
- other online services that are described in the presentations of the product for an individual client segment.

(3) The Online B@nk can be used on mobile and other devices (mobile phones, smart phones, palmtops, tablets, etc.; hereinafter Mobile Devices) that have an operating system and browser which enable Internet access.

(4) M - Online B@nk on a Mobile Device is a version of the Online B@nk that has been adapted for use on technically sophisticated Mobile Devices with smaller screens. Owing to the technical limitations of individual types of Mobile Devices, certain functions of the Online B@nk are not enabled on such Mobile Devices or the provision of a certain function is correspondingly adapted and limited.

(5) GO! Mobile Bank (hereinafter: Mobile Bank) is an application for mobile banking that allows the User to access and perform certain banking services in the Online B@nk system using software that the User downloads into their Mobile Device from Apple Store or Google Play stores or via a hyperlink they receive in an SMS. They activate the application or software using the Activation Key they receive in an SMS. In order to use the Mobile Bank, the Mobile Device that has the program installed must enable Internet connectivity. The Mobile Bank together with the M-Token and the Personal PIN Password provide the User with the latest security mechanisms with a high level of data encryption. Access to financial data and the functions of the Mobile Bank are not possible without a Personal PIN Password which is known only to the User. Additional security is provided by the data associated with the User's bank accounts never being stored on the Mobile Device and with limited-duration access to the application that shuts down automatically after three minutes of inactivity, whereby the Personal PIN Password is also automatically locked after three unsuccessful attempts at entering the PIN.

The User's existing authorisations for all accounts, for which they are authorised in the Online B@nk system or which are curtailed in accordance with the limitations and characteristics of the Mobile Bank, apply from registration in the Mobile Bank until their revocation. The characteristics and limitations of the Mobile Bank are published on the Bank's website http://www.unicreditbank.si/GO and may be amended.

The Mobile Bank can provide the following services to the User or Authorised Person:

- access to the balance and transactions on the User and Authorised Person transaction, savings and deposit accounts;
- payment card transactions and details;
- payments with a universal payment order and an internal transfer of funds between the accounts of the same User at the Bank;
- exchange rate and currency translation tool;
- archive of payments;
- other online services that are described in the presentations of the product for an individual client segment.

The applicable daily limit in the Mobile Bank is set by the Bank and published on the Bank's webpage http://www.unicreditbank.si/GO. If a lower transaction or daily limit is selected in the Online B@nk system, the lower of the two limits applies to the Mobile Bank.

IV. Method and Means of Communication

(1) In order to use the online and/or mobile banking system, the User or Authorised Person must ensure suitable computer equipment (hardware and software) or a suitable Mobile Device and communication equipment defined in the Technical Requirements. The applicable Technical Requirements for the systems are published on the Bank's website www.unicreditbank.si and represent mandatory instructions to Users regarding the method and appropriate use of online and mobile banking services as well as other important instructions for the use of online and mobile banking services.

(2) The online and mobile banking system is a closed system. Data that the Bank communicates to the User or Authorised Person via the online or mobile banking system are equal to statements in paper form that the Bank sends by mail and can replace the statements in paper form.

(3) The Mobile Bank allows the User and Authorised Person to review the sent Orders generated in the Mobile Bank, which they do under the menu item Payments Archive. Based on an Order submitted by the User via the online banking system or at the Bank's business unit, the Bank communicates to the User all of the transactions executed via the Mobile Bank, which it does on a paper or other Durable Medium.

(4) All information that the User or Authorised Person can receive from the Bank in electronic form are sent by the Bank to the User or Authorised Person in paper form only at their express request whereby

the request is made in the form of an Order submitted via the online banking system or at the Bank's business unit.

(5) A signature using a numerical password from the Token, M-Token or SMS-Token is equal to the signature in manuscript.

(6) The User or Authorised Person consents to the Bank notifying them of any changes, the Bank's new offers and special features of transacting via the online and mobile banking systems. The Bank shall specifically mark the notifications on the Bank's offer for Users or Authorised Persons.

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

(1) The Bank shall approve the use of the online and/or mobile banking system to the User if the latter:
- sends all of the required original bank forms that have been correctly filled in to the Bank;
- has a transaction account at the Bank;
- transacts with the transaction account in accordance with the General Terms and Conditions;
- settles their liabilities regularly.

(2) The Bank reserves the right not to approve the use of the online and/or mobile banking system without having to state the reasons for rejection, of which it shall inform the User in writing, whereby it shall inform the Authorised Person as appropriate.

(3) The User or the User's Legal Representative may authorise one or more Authorised Persons for use of the systems. The type of authorisation for an individual Authorised Person is determined by the User or the User's Legal Representative using the relevant bank form. The Bank performs an activation for the Authorised Person once it receives a correctly filled in bank form.

(4) The User may order the Bank to change the authorisations of an individual Authorised Person, which they do using the relevant bank form.

(5) If an Authorised Person is being granted the authorisation to sign documents digitally on line, the data on the Authorised Person must correspond with the data on the bank form entitled "Authorisation to Dispose of the Funds on the Transaction Account" of the User.

(6) The Bank may approve the Order and use of the Go! application to the Online B@nk system User based on the User's Order that was submitted via the Online B@nk or based on the application for the use of the online and/or mobile banking system that was filled in and submitted at any of the Bank's business units.

(7) The Order and activation of the service are a pre-condition for the use of the service.

(8) The agreement shall be deemed to have been concluded when the Bank approves the use of the Online B@nk system and/or the Go! Mobile Bank. application.

(9) By signing the request or agreement, the User confirms that they accept the General Terms and Conditions applicable at any relevant time.

VI. Acquisition of Means for Identification and Authentication

(1) For the purpose of entering the Online B@nk system, the User may decide on using one of the possible means for authentication; i.e. either the Token, the M-Token or SMS-Token, whereby they must take the decision on this themselves and place an order with the Bank. When they receive the Token, M-Token or SMS-Token, the User or Authorised Person assumes full responsibility for the storage of the Token and the actions resulting from the use of the Online B@nk system. The selected Token is the property of the Bank which leases it to the User or Authorised Person for the duration of the use of the Online B@nk system.

(2) If an Order is placed or an agreement is concluded for the GO! Mobile Bank service, the User or Person Authorised for the GO! Mobile Bank application receives the M-Token upon the acceptance of the application or they receive it as an independent application. After the successful activation using a Personal PIN Password, the M-Token generates a one-time limited-duration password for entry or confirmation in the Online B@nk system each time, whereby the said password uniquely identifies the authenticity of the User or Authorised Person.

(3) A Token can either be a physical password generator, M-Token or SMS-Token, which is a means allowing the identification of the User or Authorised Person and the confirmation of data when using the Online B@nk system and which is used exclusively by the User or Authorised Person. Username that the User or Authorised Person defines by themselves together with a numerical Personal PIN Password and the one-time password generated by the Token based on the Personal PIN Password provide for the unique identification of the User or Authorised Person when signing into the Online B@nk system and when confirming individual actions (payments, Orders to the Bank).

VII. Execution of Payment Orders

(1) The Bank shall be deemed to have received a payment order when the User or Authorised Person (in accordance with the prescribed rights they hold for the account) signs and send the order via the online and/or mobile banking system to the Bank's server. Information on the status of individual payment orders is provided by the Bank to the User or Authorised Person through the provision of feedback via the online and/or mobile banking system.

(2) The Bank provides the User and Authorised Person with the execution of all correctly filled in payment orders within the deadlines prescribed or agreed for an individual type of payment order in accordance with the Schedule of Transaction Account Operations (hereinafter: the Schedule). If the User or Authorised Person decides on cancelling a payment order, they may do so or communicate this via the online and/or mobile banking system in accordance with the deadlines indicated in the Schedule.

VIII. E-Invoice In the Online B@nk System

(1) The Bank makes it possible for the Users of the Online B@nk system to register for/deregister from receiving E-Invoices as well as to receive them and effect them in the form of payments in the online bank.

(2) The bank of the E-Invoice Recipient shall be obliged to:
a. accept E-Invoices that arrive in the E-Invoice Exchange system;
b. place the received E-Invoices at the User's disposal within the scope of the Online B@nk;
c. send feedback through the E-Invoice Exchange system on the delivery of the E-Invoice to the recipient.

(3) By way of the E-Registration, the User of the Online B@nk system registers for the reception of E-Invoices. The Bank sends the E-Registration via the E-Invoice Exchange system to the E-Invoice Issuer, for which the E-Registration was intended. The Bank does not guarantee that the E-Invoice Issuer will accept the E-Registration and start issuing E-Invoices to the User. The E-Invoice Issuer sends the E-Invoice through its bank to the bank of the E-Invoice Recipient, while the recipient's bank sends it to the Online B@nk. The E-Invoice Recipient may use the Online B@nk system to submit an E-Deregistration whereby they deregister from the reception of the issuer's E-Invoice.

(4) The User may subscribe for the reception of E-Invoices from issuers that are included in the E-Invoice Exchange system.

(5) Complaints arising from the contents of the E-Invoice (incorrect data, unsuitable content, wrong invoice) shall be resolved by the User directly with the E-Invoice Issuer. Complaints arising from the functioning of the E-Invoice system within the Online B@nk system shall be resolved by the Bank.

IX. Blocking or Cessation of the Use of the Online and/or Mobile Banking System

(1) With the Bank's consent, the User or Authorised Person may terminate the use of the online and/or mobile banking system without a notice period. The User or Authorised Person may terminate the use of the online and/or mobile banking system with a notice period of one month. The proposal for the cessation of the use of the online and/or mobile banking system must be submitted to the Bank using the relevant bank form.

(2) The Bank may terminate the User's or Authorised Person's use of the online and/or mobile banking system at its own discretion and with a notice period of two months, thus excluding them from the system.

(3) The Bank reserves the right to limit or terminate access to the online and/or mobile banking systems without prior notice in case of critical events (especially those related to security), if these General Terms and Conditions are not observed, in case the User does not transact appropriately and if there is a suspicion or possibility of misuse.

(4) As of the date of the termination, the Bank shall block the use of the software package and charge all of the User's or Authorised Person's unsettled liabilities in accordance with the Decision on the Payment Tariff for Retail Transactions, Transactions with Small Businesses, Sole Traders and Freelancers (hereinafter: the Tariff).

(5) All orders sent to the Bank prior to the cessation of use shall be executed in accordance with the Schedule.

(6) At the User's request, the Bank shall block the valid means of authentication for the Persons Authorised for the accounts based on the filled in form entitled Authorisations of the Authorised Person for the Online and/or Mobile Banking System.

(7) Blocking and/or exclusion of the User or Authorised Person may be performed by the Bank based on the filled in bank form entitled Application for Activation, Change or Blocking of the Online and Mobile Bank. All of the User's or Authorised Person's authorisations for the accounts listed in the form shall be blocked and/or cancelled.

(8) The Bank shall perform the blocking of services immediately after receiving the notification on the theft/loss/misuse and following the reception of all information required for blocking, and shall notify the User thereof.

(9) The Bank shall automatically block the use of the Mobile Bank application if the User enters an incorrect Personal PIN Password three times in a row.

(10) All forms must be original, signed by the User or the User's Legal Representative and their customer relationship manager.

(11) Any loss, theft or suspicion of the misuse of the means of authentication for the online and/or mobile banking system (Token, M-Token or Mobile Device) must be immediately reported by the User to the Bank, and when the case involves a User of the Mobile Bank service, they must immediately inform their mobile network service carrier of the loss or theft of their Mobile Device.

(12) The request for blocking may be submitted by the User, Authorised Person or the Legal Representative in the following ways:
- during working hours on the telephone (+386 1 5876 777 or +386 40 636 898);
- at any time via e-mail (e-mail address: e-blokada@unicreditgroup.si);
- in person during working hours at the Bank's business unit that manages their personal account. Information on the working hours is published on the Bank's website www.unicreditbank.si.

(13) The person cancelling the service is responsible for the veracity of the data provided. After receiving the notification, the Bank prevents the option of sending payment orders via the online and/or mobile banking system or blocks or withdraws authorisations of an individual User or Authorised Person for the use of the online and/or mobile banking system.

(14) The User or the Legal Representative must, within one Business Day, submit the original of the written filled in bank form on the blocking of the online and/or mobile banking system signed by the User or the Legal Representative and the customer relationship manager.

(15) The Bank shall be responsible for its own at fault actions and not for the damage or loss arising before it receives the blocking request.

(16) Payment orders submitted by the User or Authorised Person prior to the revocation of authorisations shall be executed by the Bank.

(17) The Bank shall charge the costs of a new Token to the User.

(18) Unblocking may be performed at any time based on an official letter sent by the Legal Representative or the User.

X. Obligations of the User and Authorised Person

(1) The User and Authorised Person undertake to:
- protect the software and use it only for procedures envisaged for the use of the online and/or mobile banking system;
- protect the Token, M-Token, Username, password, PIN Code and, if they use the Mobile Bank service, also the Personal PIN Password, thus preventing damage or theft;
- carefully store all means of authentication, Usernames and passwords, thus protecting them by preventing their loss, theft or misuse;
- not write down the passwords and Usernames on paper, online or other media;
- change the personal number (PIN) no less than once a month;
- regularly use the application and review data;
- regularly review the notifications sent by the Bank;
- observe the instructions for the use of the online and/or mobile banking system as well as the applicable legislation;
- immediately notify the Bank of any established irregularities or atypical functioning of the online and/or mobile banking system;
- immediately notify the Bank of eventual unauthorised use or suspicion of unauthorised use of the online and/or mobile banking system and submit the blocking request to the Bank in writing;
- notify the bank of the misuse or suspected misuse of the online and/or mobile banking system and submit the blocking request to the Bank in writing.

(2) The User undertakes to:
- immediately notify the Bank of the change or expiry of the authorisations of an individual Authorised Person;
- keep records of its Authorised Persons and their authorisations.

XI. Bank's Responsibility

(1) Upon the commencement of the use of the online and/or mobile banking system, the Bank shall provide the User and Authorised Person with all of the required elements for the use of the online and/or mobile banking system.

(2) The Bank shall provide the User and Authorised Person with uninterrupted use of the online and/or mobile banking system. Exceptions to the above shall be cases of force majeure, technical difficulties, other unexpected system failures as well as cases of the suspension of the functioning of the systems that have been announced in advance.

(3) The Bank shall not be responsible for the eventual damage arising as a result of emergencies and events that include but are not limited to: force majeure events, strikes, decisions and actions on the part of authorities, disturbances in telecommunications and other traffic, errors in the transmission of data via telecommunications networks, prevented access to the online and/or mobile banking systems services.

(4) The Bank shall not be responsible for eventual damage or loss incurred by the User or Authorised Person as a result of the malfunctioning of the online and/or mobile banking systems, the telecommunications or computer system and/or Mobile Device, which is caused by unjustified interference on the part of the User or third parties.

(5) The Bank shall be liable to the User or Authorised Person for eventual damage or loss incurred that could result from wilful intention or gross negligence on the part of the Bank. The Bank shall only be responsible

for the directly caused damage or loss. If they discover errors, irregularities or if they incur damage or loss, the User or Authorised Person shall act with the due diligence and in accordance with these General Terms and Conditions.

(6) The Bank assumes no responsibility in the event of loss or destruction of data and equipment of the User or Authorised Person arising from the installation and use of the online and/or mobile banking system.

(7) The Bank shall not be responsible for the eventual damage or loss when the User fails to keep its own records on Authorised Persons, their Payment Instruments or their authorisations for the User's accounts.

XII. Fees

(1) The Bank shall charge the User and Authorised Person for the costs of maintaining the online and/or mobile banking services in the amount laid down in the Bank's Tariff applicable at any relevant time which is published at www.unicreditbank.si. The User expressly agrees for the Bank to debit their account directly for the costs of the maintenance of the online and/or mobile banking services and other associated costs.

(2) In case the activation of the online and/or mobile banking service takes place by the 15th day of the month, the cost of the one-time registration fee and the maintenance of the online and/or mobile banking service shall be charged in the current month by directly debiting the User's transaction account, while the costs shall be charged in the following calendar month if the service is activated after the 15th day of the month.

(3) Upon the destruction, theft or loss of the means of authentication, all costs for the production of a new means of authentication shall be paid by the User or Authorised Person.

(4) We would take this opportunity to issue a special warning, i.e. that the application will be locked automatically if the Personal PIN Password is entered incorrectly three times in a row in the Mobile Bank application. The Bank shall again enable the User to transact in the system after the renewed activation of the Mobile Bank, which it shall charge the User in the amount laid down in the Bank's Tariff applicable at any relevant time.

XIII. Amicable Dispute Resolution

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

(2) The Bank shall resolve potential disputes and disagreements based on the consumer's written request. The consumer can address such request to the Bank via a prescribed form available in all the Bank's branches, in written form to the address UniCredit Banka Slovenija d.d., Šmartinska 140, 1000 Ljubljana or via web portal http://www.unicreditbank.si/pisitenam.asp. The Bank's competent body shall decide regarding the complaint in the shortest possible time or at latest within eight (8) days upon the receipt of the entire relevant documentation. The Bank shall send the answer to a complaint with adequate explanations in written format to the consumer's address. The consumer shall have the right to file an objection to a complaint. The Bank shall send the decision regarding the objection with adequate explanations in written format to the consumer'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) In case a complexity of a case shall not allow for the settlement of a complaint or objection within the stated deadline, the Bank shall inform the consumer in written format about the anticipated date of final settlement of complaint.

(4) If the user doesn't agree with the decision regarding the complaint or if they don't receive the Bank's answer to a complaint within 30 days, they shall have the right to file within maximum of 13 months from the final decision in the internal complaint procedure or from the expiration of the deadline for dealing with the complaint an initiative for the beginning of the out-of-court dispute resolution procedure with the provider of out-of-court resolution of disputes (hereinafter referred to as: the IRPS provider), who is acknowledged as competent for consumer dispute resolution by the Bank. The Bank may at any time change the IRPS providers competent for resolution of consumer disputes.

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

(6) Filing of the initiative shall not interfere with the user's right to file adequate request for dispute resolution with the court of competent jurisdiction according to the Bank's headquarters.

XIV. Transitional and Final Provisions

(1) If the Bank amends these General Terms and Conditions, it has to notify the User thereof via the online and/or mobile banking systems two months prior to their entry into force by sending the proposed amendments of the General Terms and Conditions to the User.

(2) If the User disagrees with the amendments to the General Terms and Conditions, they may withdraw from the use of the online and/or mobile banking systems without notice or payment of fees. The User must submit the request in writing no later than on the day before the date specified for the entry into force of the amendment. If the User does not notify the Bank within this time period that they disagree with the amendments, they shall be deemed to agree with them. If the User rejects the proposed amendments in writing while not terminating the use of the online and/or mobile banking systems, it shall be deemed that the Bank has terminated the Agreement with 2-months notice which starts from the day of the dispatch of the notification about the amendment.

(3) The General Terms and Conditions applicable at any relevant time shall be published on the Bank's website and in all business units of the Bank.

(4) The documents entitled Technical Requirements for the Use of the Online B@nk System and/or Technical Requirements for the Use of the GO! Mobile Bank Application, Recommendations for the Execution of Payment Transactions Via the Online B@nk and/or GO! Mobile Bank for Retail Clients at the Bank shall form an integral part of these General Terms and Conditions.

(5) All instructions relating to the use of the online and/or mobile banking systems, filling in of forms and execution of payments shall be available to the User and Authorised Person on the Bank's website and in the online banking systems under the option Help.

(6) The Bank, the User and Authorised Person agree that they shall recognise before courts the validity of each other's e-mail messages that are provided for in the software package of the online and/or mobile banking systems.

(7) The User shall have the right to demand at any time a copy of the General Terms and Conditions on paper or other Durable Medium.

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

(9) If the User detects that a violation has been committed during the provision of services on the basis of these General Terms and Conditions, whereby such violation constitutes a violation according to the Payment Services and Systems Act (ZPlaSS), they shall have the right to file a written proposal for the institution of violation proceedings. The proposal shall be filed with the Bank of Slovenia, which shall be competent for deciding on such violations.

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

(11) These General Terms and Conditions shall apply as of 13 May 2016 onwards.