UniCredit Bank Banja Luka

GENERAL CONDITIONS OF USE OF DIRECT CHANNELS OF UNICREDIT BANK A.D. BANJA LUKA

Banja Luka, 2019, July

UniCredit Bank a.d. Banja Luka
Supervisory Board

Pursuant to Article 31, paragraph 31.1, item 31.1.14 of the Articles of Association of UniCredit Bank a.d. Banja Luka number S-9/17 dated 13.10.2017, Supervisory Board of UniCredit Bank a.d. at its 6th Meeting held as at, July 30, 2019, enacted the following

GENERAL CONDITIONS OF USE OF DIRECT CHANNELS OF UNICREDIT BANK A.D. BANJA LUKA

1. SCOPE OF APPLICATION

General Conditions of Use of Direct Channels of UniCredit Bank a.d. Banja Luka (hereinafter: "**General Conditions of Use"**) set out the rights, obligations, conditions and responsibilities under which UniCredit Bank a.d. Banja Luka (hereinafter: "**the Bank**") provides to its clients legal entities and private individuals (hereinafter: "**the Users**") and private individuals authorized to use direct channels on behalf and for the account of the user (hereinafter: "**the End Users**") the use of direct channels.

2. EXPLANATION OF TERMS

The terms used in the General Conditions of Use shall have the following meaning:

- **Authorization** means a particular action or series of related actions whereby the end user on behalf and for the account of direct channel user gives consent to execute one or more financial or nonfinancial transactions, or by which he contracts on behalf of and for the account of the User one or more banking or non-banking services.
- **Direct channels** are means of remote communications which enable the use of banking and other financial and non-financial services through electronic manner of communication, without concurrent physical presence of the (End-) User and Bank employee at the same place. Direct channels encompass the network of self-service devices (ATM, day- night vault, cash deposit machine, info stand, and other types of devices) that the Bank places at the User's disposal during the contractual relationship as well as the SMS service for clients that started using the service prior entry into force of the General Conditions of Use, Internet banking, banking through mobile devices and other contracted direct channels, offering information and/or the possibility of executing financial and non-financial transactions as well as arranging banking and non-banking products and services. Direct channels are a closed system. Data that the Bank forwards to the User or End User through direct channels are equally valid within the relationship of the Bank and (End-) User, as paper print outs delivered by the Bank by mail or in any other way and can replace them. At the User's request the Bank will verify the printout of those data on paper.
- **Electronic Signature** is a set of data in electronic form which is attached to or logically associated with other data in electronic form and which is reliably guaranteeing the identity of the End User and credibility of the signed electronic document
- **Identification key** and activation key are personal identification numbers that the Bank assigns to the End User, and are used in the End User registration process for the use of certain direct channels or activation of certain means for identification and authentication.
- **User manual** is a written document available on the Bank's web page (http://www.unicreditbank-bl.ba), which describes the User and/or End User registration method for using an individual direct channel, the way of using a direct channel, banking and non-banking services that can be performed by the User using one or more direct channels, and the method of their performing.
- **User number** is a unique set of alphanumeric characters constituting one of the elements by which the End-User is identified in the registration process for particular services of direct channels.
- **User** is a legal entity or private individual that contracts with the Bank usage of some of the direct channels.
- **End User** (Authorized person) is a private individual authorized by the User for using a particular direct channel for and on behalf of the User.

- **Smart card and USB key** are certified cryptographic devices for secure electronic certificate storage.
- **Personalized security features** are secret identification numbers that are known only to the end user and are considered to be initial PIN, PIN, identification key, activation key and unlock code/password.
- **PIN** is a personal secret end user identification number, known exclusively to the end user, and is used to identify the end user for access to a smart card/USB key or other identification and authentication device that can be used after the correct PIN entry
- **Business entity** is a legal entity and part of a legal entity, company, public company, bank or other financial organization, an association, a public institution, an administration body, a body of local self-government unit or any other form of organization whose establishment is registered with the competent authority or is based on regulations, as well as a natural person who independently performs a registered business activity.
- **Signatory** is the End-User who owns the device for the creation of the electronic signature (USB key or smart card) with which he signs, and acts for the User on the basis of the granted authorities.
- **Certificate** is a confirmation in electronic form, issued by the Bank, with limited validity term, stored on the smart card or USB key that links the data for electronic signature verification with the End-User to which the Bank assigned the concerned USB key or smart card, and confirms his identity.
- **Identification and certification means** is a device or application solution that provides end user identification for access to direct channels, contracting services, and giving approval to the execution of payment orders and other types of orders that are issued by using direct channels. The identification and authentication device may be different depending on the direct channel used (account card, USB key, smart card, or any other identification and authentication device that the Bank assigns to the user or end user).
- **Unlock code/password** is a code/password used to unlock smartcards or USB Keys in the event when a smartcard or USB Key is locked due to successive entries of a wrong PIN.
- **Durable data carrier/durable medium** is any instrument that enables the User to store data so that they are available for later use for as long as is necessary for their intended use and that allows unchanged reproduction of stored data
- **Contract** is a contract for the use of a specific direct channel, concluded between the Bank and the user.
- **Manual for use of identification and certification means** is a written document, available on the Bank's web page ((http://www.unicreditbank-bl.ba), which describes the method of activation and/ or use of one or more identification and certification means.
  The Virtual card is a functionality of a card whose issuer is the Bank, which enables the Card User being at the same time the User of the mobile banking application to perform the contactless payment transactions with the card at acceptance points in Bosnia and Herzegovina and abroad that accept the contactless payments supported by the mobile banking application he/she previously installed and activated on a mobile device.

3. GENERAL PROVISIONS

Information on the offer of direct channels and services that a user can make using certain direct channels is available in the Bank's business network and on the Bank's web page (http://www.unicreditbank-bl.ba).

For any agreed direct channel, the Bank will provide the User with insight into all reasonably necessary information and execution of transactions within the scope and in the manner specified in agreement and/or User's manuals for the particular direct channel

The Bank reserves the right to change the contents of the relevant direct channel, of which it notifies the User in writing via SMS, e-mail of via other communication medium, which presents the agreed communication means with the client.
All changes in the scope and contents of a particular direct channel will be available to the User at Bank's branches, as well as at the web-page (http://www.unicreditbank-bl.ba).

The user is not entitled to claim damages for changes to the user manual, instructions for use of identification and authentication device, or services that can be performed using the contracted direct channel.

The Bank is authorized to introduce new and modify existing forms used for contracting or when using certain direct channels, and which constitute an integral part of the contract, and it will publish them on the Bank's web page (http://www.unicreditbank-bl.ba).

To use particular direct channels, the User must ensure appropriate computer (hardware and software) and communication equipment. Technical requirements for the use of individual direct channels have been released on the Bank's web page (http://www.unicreditbank-bl.ba) and/or are available in the Bank's business network. If the User is using type of equipment different from specified technical requirements of the particular direct channel, they are required to inform the Bank on the type of equipment used in order to ensure proper correct functioning of the direct channel.

The User is responsible for all information submitted to the Bank, necessary for the proper and safe functioning of the contracted direct channel and they are also required to update and inform the Bank of any change thereof (e.g. phone number, e-mail address, etc.).

The data forwarded by the Bank to the user or the end user via direct channels are as valuable as the paper printouts sent by the Bank by mail and may replace them. At the request of the user, the Bank will certify the printout of this data on paper. The Bank will allow the user to store and / or print data on services performed using direct channels, so that they can be available for later use in a period appropriate to the purpose of the data and to enable the reproduction of the stored data to them.

4. CONTRACTING OF THE DIRECT CHANNELS

The condition for the conclusion of the contract is that the user opens a transaction account at the Bank, or use some other product or service for whose use the direct channel whose contracting he requests is envisaged.

The User may contract use of one or several direct channels in the way regulated for individual direct channel by the General Conditions of Use and/or appropriate user manual.

To contract individual direct channels, the user must submit to the Bank a properly completed and signed form envisaged for the contracting of that direct channel. By signing a direct channel contracting form, the user confirms that he is familiar with the General Conditions of Use and other acts applied together with them, and agrees to their use.

The User can designate one or several end users who will use on his behalf the contracted direct channel. For internet banking, the user must choose one type of authorization to each end user, or a combination of several types of authorization, between those offered to him by the Bank.

For individual End User it is possible to choose different types of authorization. The choice, change and revocation of authorizations of the end users are based on the delivery of properly filled out forms of the Bank envisaged for individual or several direct channels and which the End User submits to the Bank in the manner envisaged for a particular direct channel.

By signing Agreement on Use of the Direct Channel, the User will grant the consent that the Bank is authorized by the General Conditions of Use and/or appropriate user manuals to introduce new types of authorization, to change the scope of certain types of authorization, or to terminate certain types of authorizations that the user selects for the end users.

All forms provided by the user to the Bank in connection with the contracting, using and termination of the use of the contracted direct channel must be signed by the user or a person authorized to represent the user and verified by the stamp reported to the Bank by the User.

Use of particular direct channel is contracted by the User and the Bank by signing an agreement or other form appropriate for contracting (e.g. Application Form).

For a single direct channel, the User may use at least the first working day after the conclusion of the contract and take over or provide the user and / or end user with all necessary personalized security features and / or identification and authentication device necessary for the use of that direct channel.
The User can use a particular direct channel no later than on the first business day after the conclusion of the contract and taking over or delivery to the user and/or end user of all necessary personalized security features and/or identification and authentication devices, necessary for the use of that direct channel.

5. SECURITY

The Bank will assign the contracted identification and authentication device and/or personalized security feature to the End User when that is necessary for use of one or several contracted direct channels.

The identification and authentication device provided by the Bank to the User or End User is owned by the User if he has paid the Bank's appropriate remuneration for the device in question.

The User is obliged to use the Identification and Authentication Device in the manner prescribed by the Bank's Instructions for the use of the direct channel, to which they are related.

To the End User who uses the USB Key and/or smart card as identification and authentication device the Bank will assign an initial PIN, which is used in the End User registration process for the appropriate direct channel service. The End User is required upon the implemented registration process and before the login in the appropriate direct channel, to select and confirm the PIN, with which he will be further identified for access to the certificate on the USB Key or smart card.

If the end user has not received or forgot or lost the assigned initial PIN, or has lost or forgot the PIN with which he accesses to the assigned identification and authentication device, the Bank will re-assign the new PIN to him on the basis of properly filled out appropriate Bank forms signed by the user and/or end user.

In the event of loss, theft, locking or damage of the identification and authentication device, or the replacement of the identification and authentication device by the same or other identification and authentication device, the Bank shall issue the new identification and authentication device to the user i.e. end user upon receipt of the corresponding properly filled out form.

The security aspect of dealing with the contracted identification device is specified in detail in the item 13 (OBLIGATIONS OF THE USER).

6. ORDERS FOR EXECUTION OF PAYMENT TRANSACTIONS

Depending on the type of direct channel by which the payment order is assigned and/or the type of identification and authentication device used by the end user, the consent to execute the payment transaction using the direct channels is given in one of the following ways:

a) by electronic signing an individual payment order or a file with payment orders using the certificate on the USB key or smart card, in the event that the user authorized for payment orders signing jointly two/more end users who use USB Key or smart card as identification and authentication device;
b) by electronic signing an individual payment order using the certificate on the USB Key or smart card, in the event that the user authorized for payment orders signing independently one end user each, who uses USB Key or smart card as identification and authentication device;
c) by electronic signing the file with payment orders using the certificate on the USB Key or smart card, if the user authorized for payment orders signing independently one end user each, and file was sent through the appropriate direct channel for execution by the end user who is different from the end user who signed the file;
d) using the account card on the ATM with identification through assigned PIN on the account card and selecting appropriate option for cash depositing/withdrawing on the device itself;

e) using the card for day-night vault and selecting appropriate option on the device itself performs the deposit of security PVC bag;
f) other contracted ways for individual direct channels.

A payment transaction for whose execution the approval has been given in one of the above ways is authorized. Use of personalized security feature and identification and authentication device is considered unambiguous evidence of identity of the User or End User and their confirmation of payment transaction. The fact that the Bank as a use of a payment instrument recorded the use of the identification and authentication device accessed by a personalized security feature will be sufficient to prove that the user i.e. the end user has authorized the relevant payment transaction by which the user assumes responsibility for the executed relevant transaction.

The methods, assumptions and effects of authorization of payment transactions under this item of the General Terms of Use, depending on the type of identification and authentication device, and the selected number by the user of end-users for the signing of the payment order, apply in an appropriate way to the performance, assumptions and effects of other financial and non-financial transactions and contracting services using direct channels.

The Bank will immediately upon the receipt of the payment order, through the same direct channel by which the payment order was given, deliver the message on successful acceptance of order to the User/End User. The message of successful acceptance of a payment order does not imply that the payment order will be executed, but only that the Bank has received it.

The Bank executes the correct payment orders within the deadlines prescribed or agreed upon for certain type of payment order, in accordance with the transaction execution time on the accounts of the users valid at the moment of the payment transaction execution.

The Bank, in order to monitor and verify the correctness of the issued payment orders (taking into account the certain restrictions set by regulations, legislation, reasonable suspicion of the abuse of a direct channel, etc.) through direct channels, has the right to temporarily keep the payment order issued and to provide additional documentation/ information from the user. In the event that the verification establishes the correctness of the issued order or the additional documentation required for the execution of the order is provided, the Bank executes the order according to the valid times for execution of transaction on user's accounts at that moment. If the order has been issued before the execution time of the order with the current value date, and the process of additional verification of the correctness of the issued order or the collection of additional documentation completed after the defined time for the particular type of transaction, the Bank will execute the order with the date of the following business day.

Payment orders that are given by direct channels before the execution value date by can be revoked by the user and the end user until the execution value date that was determined by the valid time to execute transactions on user accounts in that moment. Payment orders can be revoked using the same or another direct channel that allows submission and revocation of payment orders in accordance with General Business Conditions for Operations with Private Individuals of UniCredit Bank a.d. Banja Luka (hereinafter: "**General Business Conditions for Private Individuals**") and General Business Conditions for Operations with Legal Entities and Entrepreneurs of UniCredit Bank a.d. Banja Luka (hereinafter: "**General Business Conditions for Legal Entities**") and other internal acts of the Bank.

The Bank may refuse to execute a payment order in accordance with the legal and subordinate regulations and the General Conditions of Use.

The Bank will not be held accountable for non-execution of payment transactions or for erroneous execution of payment transaction via direct channels, which would happen due to incorrectly inserted data into the respective order by the User i.e. End User.

7. VIRTUAL CARD PAYMENTS

Via mobile banking application, the User can choose the cards which, besides in physical form, can also be used in the form of a virtual card, the use of the virtual card selected in the manner, selection

of, and the change in settings of use of the selected virtual card, as well as sending of notification of payment transactions and expenses made by using the virtual card.

Virtual Card can be used by the User who has agreed on use of the mobile banking application and to whom the Bank has issued a card with the possibility of activation of the virtual card function.

The User can use the virtual card after he/she has installed on a mobile device an updated version of the mobile banking application which supports the card digitalization service, and then, using the mobile banking application, after entry of the PIN which the User selected for access to the mobile banking application, chose the card, whose User he/she is and in which the Virtual Card function can be activated, and then activated the virtual card selected in the manner, all in the manner specified in the User Instructions that can be found on the web page of the Bank www.unicredit-bl.ba . Within the scope of the mobile banking application, the Bank will show the User all valid cards, it has issued to him/her, and in which the User can activate the Virtual Card function. The mobile device which the User will use to access the mobile banking application and use the virtual card must meet all conditions set in the User Instructions for the use of the virtual card, which also includes User's obligation to previously adapt and activate, on that mobile device, all security settings prescribed by the User Instructions.

By selection and activation of the selected virtual card, the User confirms that he/she is aware of the fact that the use of the virtual card is associated with an increased risk of execution of payment transaction by unauthorized person, which can occur in case of loss, theft, or misuse of a mobile device, on which the mobile banking application has been installed with the Virtual Card activated and in function. The Virtual Card is used without entry of PIN which the User selected to access the mobile banking application and without entering the card's PIN on the POS device up to the amount of 30.00KM, defined by the rules of the MasterCard card company, i.e. without signing the User's slip.
For the payment amounts over 30.00KM, entering the card PIN is mandatory, PIN of the mobile banking application is entered during the payments .

If the User, who has an active mobile banking application and an active virtual card, requests blocking of the mobile banking service, the Bank is authorized to disable the access and / or use of the virtual card / cards that is/are active in the mobile banking application. The User to whom the Bank has disabled the access to, and/or usage of the selected Virtual Card, can still use the subject card issued to him/her in the physical form, in line with the Bank's General Business Conditions with Private Individuals that stipulate the use of the card with the activated function of the Virtual Card. If the Bank enables the User to choose a virtual card, the chosen virtual card will be included in the mobile banking application, which the User installed on the mobile device, and it will be visible to the User within the application.

The Bank is authorized, by changing the User Instructions, to alter the manner of selection, activation, and use of the virtual card, the settings for use of the virtual card, as well as the necessary or recommended configuration of the mobile device required for use of the virtual card, whereas it will notify the User about those changes at the Bank's branch offices, via Bank's Internet page www.unicredit-bl.ba. It is deemed that the User has accepted the changes in the User Instructions if, after their entry into force, he/she has used the virtual card i.e. mobile banking application.

The virtual card can be used for payment of goods and/or services at points of sale in Bosnia and Herzegovina and abroad, which display the sign of contactless cards acceptance.

The User grants the consent to execution of a payment transaction initiated by use of the virtual card by moving closer the mobile device, on which the mobile banking application with the included and activated Virtual Card, and the included NFC option on the mobile device the POS device accepting the contactless cards, and additionally, in the case that a payment transaction exceeds the amount set by the rules of the MasterCard company, by signing the User's slip or entering the card's PIN on the POS device. With the mobile banking application, the User can select that the virtual card can be used after the mobile device, on which the mobile banking application has been installed with the included and activated Virtual Card, has been turned on along with the display on, or, in the case that the User wants to increase his/her security, after the mobile device has been turned on and unlocked. The consent to execution of a payment transaction or a series of payment transactions, granted by use of the virtual card, cannot be revoked i.e. only exceptionally, in case of agreement between the Card

User and/or the Bank and/or the point of sale. For such revocation, the Bank is entitled to charge a fee, if it has had the expenses related to the transaction revocation. The Bank will inform the User about successfully executed payment transaction, initiated by use of a virtual card, through the mobile banking application.

To the use of the Virtual Card, the same daily limit for performance of payment transactions is applied, which is related to the card with the activated virtual card function. The expenses made by use of the virtual card are deemed expenses made by use of the card with activated virtual card function.

The responsibility of the User for expenses arising out of misuse of the virtual card, which are the consequence of loss, theft, or misuse of the mobile device, on which mobile banking application has been installed with the included and activated virtual card, is subject to provisions on the User's responsibility for the expenses that come from misuse of the card from the General Business Conditions with Private Individuals. In that sense, the loss, theft, or misuse of the mobile device on which mobile banking application has been installed with the included and activated virtual card are treated identically as loss, theft, or misuse of the card with the activated virtual card function.

Irrespective of the rules from the previous paragraph of these General Business Conditions with Private Individuals, for a payment transaction executed by use of the virtual card which is proven not to be authorized by the User and that it is a consequence of use of a lost or stolen mobile device on which mobile banking application has been installed, or consequence of the other misuse of the mobile banking application which had been carried out before the Bank was notified of the loss, theft, misuse, or suspected misuse of the mobile device on which the mobile banking application has been installed and/or before the Bank was notified of the loss, theft, or misuse of the User's personalized security features, i.e. before the Bank was informed about the knowledge or suspicion that unauthorized person had had access to the mobile banking application, the User is also held fully accountable, i:

a) if he/she failed to meet or breached any of the obligations from the Article 14 of these General Business Conditions
b) if he/she made it possible for other persons to use the agreed mobile banking application or the mobile device on which the mobile banking application has been installed with the activated application
c) in case of change of the security settings of the mobile device on which the mobile banking application has been installed with the activated application, thus the security level of the use of the mobile banking application and/or the virtual card decreased
d) if he/she failed, without delay and immediately upon becoming aware of, to inform the Bank in accordance with these General Business Conditions about any circumstances which in line with these General Business Conditions, represents the basis for blocking of the access to the mobile banking application
e) in the case of the fraud by the User.

The User can, with the mobile banking application, disable and then re-enable the use of every virtual card, for which the subject function was previously activated. The User can request the Bank to block the virtual card function in all or certain cards that the Bank issued to him/her. The main user can request the Bank to block the virtual card function in any card that the Bank issued to the additional user. The User submits request for blocking the virtual card function to the Bank on the telephone number that will be available on the Bank's Internet page www.unicredit-bl.ba, or at Bank's branch offices by submitting the written request. The Bank is authorized to disable the use of the virtual card in the case any condition has been fulfilled for blockage of the use through a direct channel specified in these General Business Conditions and/or any condition for the card blocking set forth in the applicable General Business Conditions with Private Individuals that stipulate the use of the card with the activated virtual card function. The impossibility of use of a virtual card does not affect the possibility of use of that card issued to the User in a physical form. Blockage of use of a card issued to the User in physical form disables its use in the form of the virtual card.

The virtual card can be used until the expiry date of the card with the activated virtual card function. By the validity expiry of the card, with the activated virtual card function, the possibility to use the stated card in the form of the virtual card also ceases. In case of renewal and/or replacement of the card, without change of the card number, with the previously activated virtual card function, the renewed

and/or new card automatically retains the virtual card function, without the need for the User to reactivate that function.

8. DISPOSAL OF FUNDS

The User disposes with all funds on accounts opened based on concluded agreements for which use of individual direct channel is envisaged, up to the amount of available amount of funds on the account, including permitted overdraft as well.

9. BLOCKING AND CLOSING OF DIRECT CHANNELS

The loss, theft, suspicion of misuse, or misuse of identification and authentication device, certificates stored on the identification and authentication device or personalized security features, knowledge or suspicion that an unauthorized person has learned personalized security features, and the knowledge or suspicion that an unauthorized person had access to the contracted direct channel, the user and / or end user must immediately report to the Bank and request blocking of the access to the direct channel, by calling the telephone numbers listed in the relevant user manuals, on the Bank's web page and/or the relevant direct channel, and confirm the report in writing at the latest on the following business day. The Bank will act appropriately either upon the report by the user or upon the report by the end user.

The user and the end user, independently of the obligations under this item, are obliged to change the PIN independently without delay, if they have any knowledge or suspect that the unauthorized person has found out the PIN.

Reporting the loss or theft of the identification and authentication device on which the certificate is stored is the basis for revocation of the certificate. The Bank is obliged to revoke the certificate within sixty (60) minutes from the moment of the receipt of the report.

The Bank will also automatically disable access to the direct channel using the assigned identification and authentication device even without the report by the user or end user, if the personalized security feature has been repeatedly entered incorrectly a certain number of times (according to the corresponding user manuals) depending on the device and the identification device used.

The Bank is authorized, even without the report of the user i.e. end user, to disable access to individual or all direct channels, in cases of:

a) Suspicion in unauthorized use or misuse of identification and authentication devices or personalized security features;
b) Suspicion that the direct channel is used for fraudulent acts or misuse.

The situations which are beyond the Bank control and which the Bank cannot prevent, or have influence on them, will justify the suspicion of possibility of direct channel abuse, when, according to justified and reasonable Bank assessment, security of personalized security features and/or information security of uncertain number of Users is endangered in such extent that temporary blocking of access to direct channel to individual or all Users represents the only reliable measure that can prevent loss to Users.

In the event that the user i.e. final user does not renew in a timely manner the certificate stored on the identification and authentication device assigned to the end user, the Bank shall temporarily until the renewal of existing or issuing of the new certificate disable the access to that end user to the contracted direct channel using the assigned identification and authentication device.

In cases when conditions for blocking of access to direct channel are met, the Bank can instead of blocking the access to direct channel temporarily disable use of one or several services that are accessible through that direct channel.

The Bank, on the basis of a diligent assessment of all circumstances, assesses whether the conditions for blocking access to a particular direct channel or for disabling the use of one or more services through a particular direct channel are met.

The Bank shall notify in advance the user and the end user of the intended blockage of the direct channel access and/or the inability to use the particular service via the direct channel and the reasons for such action, unless the disclosure of such notice is contrary to objectively justified security reasons or against the regulations. The Bank is not required to notify in advance the user and/or the end user of the blocking of access to the direct channel in case of an incorrect entry of a personalized security feature, or the expiration of the validity period of the certificate stored on the identification and authentication device assigned to the end user. The Bank sends the notification of the inability to use a direct channel or individual service available through the direct channel to the user and the end user via the same direct channel or in some other appropriate way.

All payment orders received by the Bank prior to the implemented revocation of the certificate or the blockage of access to the direct channel will be executed.

The Bank may with an announcement at least 24 (twenty-four) hours in advance, temporarily disable the use of contracted direct channels in case of changes or upgrades of the Bank's information system, including its information security system, or in case of changes or upgrades of the direct channel. The Bank sends the notification of temporary inability to use direct channel to the User and/or the End User via the same direct channel, by posting it on the Bank's web-page (http://www.unicreditbank-bl.ba) or in any other appropriate way.

The Bank will, after termination of the reasons for which the user was blocked access to a particular direct channel or he was disabled from using certain services within a particular direct channel, except in the case of a change/ upgrade of the information system/ direct channel, only upon his request to enable access to that direct channel and use of related services.

If the user wishes to continue using that direct channel after the reasons terminated for which his access to another channel had been blocked, he has to re-agree its use with the Bank or submit a written request for re-use, except in the case of a change/ upgrade of the information system/ direct channel.

For the costs of the new identification and authentication device, that has to be delivered to the user/ end-user in order to enable the continued use of the direct channel, the Bank can charge the user in accordance with the Bank's relevant decisions regulating the tariffs of fees for services in operations with legal entities and/or private individuals.

The User can in agreement with the Bank cancel the use of direct channel without notice period, in the way regulated for a particular direct channel. As of the date of cancellation the Bank blocks the use of direct channel and calculates all unsettled liabilities of the User in accordance with the relevant decisions of the Bank regulating the tariffs of fees for service in operations with legal entities and/private individuals, and all orders sent to the Bank before the use termination will be executed.

10. COMPLAINTS

The user of direct channels, for all complaints related to the use of direct channels, contacts his contact person in the Bank or organizational unit of the Bank responsible for customer support. If the User of Direct Channels deems that the Bank does not comply with the obligations from the concluded contract, good business practices, Bank’s General Business Conditions, provisions from Laws, they can address the Bank with a written or verbal complaint. The written complaint can be sent to the Bank directly by sending it by mail to the Bank’s address, or electronically to the e-mail address of the Bank recitenam@unicreditgroup.ba, and, in accordance with the Bank’s internal procedure of the way of dealing with the Client’s complaint. If the User of Direct Channels complains verbally, and is not satisfied with the Bank’s response, the Bank is obliged to inform them on the right to submission of the written response

The Bank is required to respond to the User to the complaint within 30 (thirty) days from the date of complaint receipt.

In case that the User is not satisfied with the answer of the Bank to the submitted complaint i.e. with the result of the process related to the complaint applied by the Bank, or the Bank does not submit the response within the stipulated term of 30 days, the User is entitled to notifying about that and filing the complaint against the work of the Bank to the Banking Agency of Republic of Srpska, or the Ombudsman for Banking System within the term of 6 months from reception of the response i.e. expiry of the term of 30 days if the Bank has not submitted the response
The Bank cannot charge the User any fees or any other expenses for submitting and handling the complaint.

11. FEES

For contracting of direct channels the User pays the fee for direct channel contracting which the Bank is authorized to collect automatically from the User's account and in accordance with the corresponding decisions of the Bank which regulate the issues of tariffs of fees for services in operations with legal entities and/or private individuals valid at the time of contracting.

For the use of direct channels, the user pays the usage fee that the Bank is authorized to charge automatically directly from the user's account without his further questioning and consent.

For direct channels which provide the possibility to perform payments, the fee is charged for individually performed payments, in accordance with the corresponding decisions of the Bank which regulate the issues of tariffs of fees for services in operations with legal entities and/or private individuals valid at the time of making payment.

For contracting products or contracting performance of other services through direct channels the fee is charged as stipulated by the corresponding decisions of the Bank which regulate the issues of tariffs of fees for services in operations with legal entities and/or private individuals valid at the time of contracting.

In the event of theft, loss or damage of the assigned identification and authentication device, the issuance of a new identification and authentication device or the issuance of a new initial PIN i.e. PIN, the Bank will charge the fee for issuing and/or actual costs of issuing the identification and authentication device or i.e. new PIN, in accordance with the corresponding decisions of the Bank which regulate the issues of tariffs of fees for services in operations with legal entities and/or private individuals valid at the time of carrying out the activity in question.

The Bank can also charge fee for other transactions executed by the User through the direct channels, in accordance with the corresponding decisions of the Bank which regulate the issues of tariffs of fees for services in operations with legal entities and/or private individuals valid at the time of transaction carrying out.

12. METHOD AND MEANS OF COMMUNICATION BETWEEN THE USER AND THE BANK

To use the system of direct channels, the User must ensure appropriate computer (hardware and software) and communication equipment which is specified in the technical requirements of a particular direct channel. Valid technical requirements for individual direct channels which require them have been released on the Bank's web page (http://www.unicreditbank-bl.ba). If the User is using type of equipment different from specified technical requirements of the particular direct channel, they are required to inform the Bank on the type of equipment used in order to ensure proper correct functioning of the direct channel.

The User is responsible for all contact information submitted to the Bank, and which are necessary for the proper and safe functioning of individual direct channel and they are also required to regularly update and inform the Bank of any change thereof (phone number, e-mail address, etc.).

The User agrees to be informed by the Bank on all changes, news in the Bank's offer and specificities in the operations via system of direct channels.

13. PROTECTION OF DATA AND CONFIDENTIAL INFORMATION

The Bank keeps as confidential all data, facts and circumstances on individual user and end user which it comes into possession of. By signing the consent to processing , the User grants the consent to the Bank that the personal data can be entered into documentation which is created for the purpose of exercising rights and obligations from the contractual relationship. The Bank is required to handle the mentioned data consistent with the legal obligation of keeping the secrecy of data which it came into possession of in doing business with the User, ensuring confidential treatment of such data and full protection of the business and banking secret on the side of all persons that will be granted access to the protected data, as well as their use exclusively for legal purposes and not in any way that might be considered contrary to the interests of the contracting parties.

14. OBLIGATIONS OF THE USER

In the event that when using direct channels, the address of the Bank does not start with http://www.unicreditbank-bl.ba, the User/End User is not on the Bank's web page, and in that case without delay, he must stop using the assigned identification and authentication device with which he accesses the corresponding direct channel, so that without delay he pulls out the USB Key from the computer i.e. the smart card from the reader. By clicking on the padlock icon next to the address bar in the browser, the user/end user must check when accessing the direct channel, as well as during use of the corresponding direct channel, whether he is on the Bank's web page.
The User and End User are obliged to:

- take all reasonable measures to protect the secrecy of the assigned identification and authentication device and/or passwords, whereby the user or the end user will not be deemed to have taken the necessary reasonable security measures, e.g. if they choose a combination of numbers, letters or characters that can be easily identified as they password (e.g. the name of the user or the end user or members of his family, the end-user's date of birth or an uninterrupted series of consecutive numbers) or, if they do not change the previously selected PIN/ password within reasonable deadlines.
- to carefully keep the assigned identification and authentication devices, so to prevent their damage, loss, theft or misuse.
- To use assigned identification and authentication devices in the manner defined by the appropriate user manuals and any possible subsequent notification by the Bank to the user and/or end user for the use of the identification and authentication devices.
- To carefully and with due care keep own devices used to access a direct channel (e.g. computer or account card) so as to prevent their loss, theft or misuse.
- To carefully and with due care protect the identification and authentication device of the Bank and use it in accordance with the General Conditions of Use and the appropriate user instructions.
- To carefully and with due care keep the identification and authentication devices and/or passwords, so as to prevent their loss, theft, misuse or unauthorized disclosure.
- Not to write down personalized security features (e.g. password, PIN) on paper, electronic or other media, nor communicate them to third parties, including the Bank and its employees, with both the user and end user being informed of the fact that the Bank and its employees will not request in any case data on their personalized.
- To act in accordance with the General Conditions of Use, the corresponding user instructions and other Bank regulations governing the use of the corresponding direct channel and the use of the Bank's products that are performed through that direct channel.
- To regularly check the existence of new information and act in accordance with the information made available to him and/or the end user by the Bank via electronic banking and/or web page (http://www.unicreditbank-bl.ba).
- For access to direct channels, use exclusively the computer equipment (hardware and software) that is compliant with the recommended configuration, and which has installed, updated and upgraded, in accordance with all available upgrades, operating systems with the associated firewall, internet browser and antivirus protection.
- To comply with all safety measures for the protection and use of computers they use to access the direct channel, which are recommended to them by the Bank, including:
  a) protection of computer access with confidential password:

b) selecting for the password/code such a combination of letters, numbers and characters that cannot be easily discovered;
c) regular periodic change of the selected password;
d) protecting the secrecy of the selected password to prevent its disclosure and unauthorized use;
e) not opening electronic mail messages (e-mails) and attachments received from unknown or suspicious senders, and links from such messages;
f) obtaining hardware equipment and software applications from secure and verified sources;
g) taking care of web pages visited from devices used to access direct channels because access to some inappropriate sites involves an increased risk of infecting computer with malicious programs;
h) regularly daily updating of anti-virus definition and scanning of all applications on computers used to access direct channels with an updated antivirus program.

- to take out the relevant identification and authentication device and computer and/ or other used equipment, and immediately after termination of the service performing by using direct channels.
- to timely renew certificate stored on the assigned identification and authentication device.
- to inform the Bank on all established irregularities and/or atypical functioning of direct channels, and immediately after determining.
- to inform the Bank about the occurrence of any circumstances that, in accordance with the General Conditions of Use, constitute the basis for blocking access to the contracted direct channel and to require the Bank to block access to the direct channel immediately upon the occurrence of such a circumstance.
- to report to the police and/or other competent authority/body the theft or misuse of the identification device and/or personalized security features, and the knowledge or suspicion that the unauthorized person had access to the contracted direct channel without delay.
- to submit to the Bank a copy of the criminal and/or misdemeanor report filed or the competent authority's acknowledgment of its receipt, without delay.
- to inform the Bank on changes to all data of the user and/or end user, such as change of the name, seat or persons authorized to represent the user, i.e. change of name and address of the end user, immediately upon the occurrence of the mentioned changes.

15. RESPONSIBILITIES OF THE BANK

The Bank shall ensure the availability of certain direct channels within their working hours determined by the user manual and/or the times for execution of transactions on user accounts, i.e. the uninterrupted availability of those direct channels for which it is provided like that by corresponding user manual and/ or times for execution of transactions on user accounts, except in cases envisaged by the General Conditions of Use, as well as in cases of force majeure, technical difficulties, and other unexpected events.

The Bank shall not be liable for any damages incurred prior to the user's report on loss, theft, unauthorized use, misuse or suspicion of misuse of the identification and authentication device or personalized security features, or before the user’s report on knowledge or suspicion that an unauthorized person has learned personalized security features or had access to direct channels, as well as for damage incurred prior to the expiration of 60 (sixty) minutes from the moment of the concerned report.
The Bank is not responsible for damages that the User/ End User incurred due to:

- Failure by the user/end user to adhere to the agreement, General Conditions of Use, corresponding user manuals and other Bank acts regulating the use of direct channels and/or Bank products that are performed via direct channels, as well as possible subsequent notifications of the Bank to the user and/or end user for use of the identification and authentication device.
- Failure by the user/end user to adhere to the last security instructions provided by the Bank on its web page, or provided to the user by a contracted direct channel or other contracted communication channel.
- Fraud or other unlawful action by third parties to the detriment of the user or end user, and which occurred as the consequence of failure by the user/end user to adhere to the

agreement, General Conditions of Use, corresponding user manuals and other Bank acts regulating the use of direct channels and/or Bank products that are performed via direct channels, as well as possible subsequent notifications of the Bank to the user and/or end user for use of the identification and authentication device.

- Termination of the validity of the certificate stored on the identification and authentication device assigned to the user and/or end user.
- Misuse of identification and authentication devices used by the user and/or the end user to access the direct channel.
- Lack of functioning or improper functioning of a computer or other device that is not owned by the Bank, and it is used to access a direct channel or malfunction or improper functioning of the application solution installed on that device.
- Intervention of the user, end user or other unauthorized person on the assigned identification and authentication device.
- Action or omission of the person that provides to the user and/or end user and/or the Bank the services of mobile and/or fixed telecommunication (e.g. internet connection).
- Force majeure, whereby the force majeure are considered especially war, riots, terrorist acts, natural disasters, epidemics, strike, power outage, interference in the telecommunication and other traffic, errors occurred in the transfer of data via telecommunication networks, decisions and actions of the authorities, as well as all other similar circumstances whose occurrence cannot be attributed to the Bank i.e. that are beyond the control of the Bank and due to which the use of a direct channel has been disabled.

The liability of the Bank for the damages resulting from ordinary negligence of the Bank, its employees or third parties engaged by the Bank to act in fulfilment of its obligations is excluded.
The Bank is only liable for the ordinary damage. The Bank shall not be liable for missed benefit, non-material damage, loss, destruction or change of user and/ or end-user data, as well as for any damage caused to the computer equipment from which contracted direct channel is being accessed to.

By signing the consent to the personal data processing, the User accepts that the direct channels, depending on their type, include data transmission via telecommunications connections (wired and wireless - for the Internet, telephone or GSM device), and are therefore associated with risks that are common to use these ways of communication. The Bank guarantees to the User that the communication via e-ba /m-bank / HALCOM/e-ba Plus solutions is protected

If for certain versions of operating systems and internet browsers the manufacturer stops providing services of upgrading and updating security components which could result in a substantial breach of security, the Bank may stop providing the direct channel service on identified operating system and internet browser with prior notice to the User and/or End User.

16. OTHER PROVISIONS

By signing Agreement on use of certain direct channel, the User confirms that they are informed of the General Conditions of Use, that the mentioned document has been furnished to them, that they have read and understood them, and that they agree to their application.

The Bank and the User agree that they will, in accordance with the relevant regulations, mutually recognize in the court the validity of the electronic messages that are provided within certain direct channels.

The General Conditions and their amendments are available to all Users and all clients of the Bank at all Bank's business premises where it operates with clients as well as on the Bank web-page (http://www.unicreditbank-bl.ba). The User has the right, at any moment, to request a copy of the valid General Conditions of Use in hard-copy or another durable data carrier.

The Bank reserves the right to amend the General Conditions of Use. Amended General Conditions of Use bound the User if the Bank, within 15 (fifteen) days from the day the User received the notification on amendments, does not receive User's notification of non-acceptance of modified General Conditions of Use. If the User of direct channels does not accept amendments to the General Conditions of Use, they are required to close the contracted direct channel i.e. within a further period

of 30 (thirty) days to cancel i.e. terminate the existing contractual relationship without paying extra costs.
All instructions related to the use of direct channels, filling-up and conducting payment as well as transfer are available to all Users at all business premises where Bank operates with clients, and at the Bank's web-pages (http://www.unicreditbank-bl.ba).
All disputes occurred during or in relation with use of direct channels, the User and the Bank will solve amicably. Should that not be possible, the competence of the court in Banja Luka is agreed, for the foreign user as well.
These General Conditions of Use are applied together with the General Business Conditions for Operations with Legal Entities, General Business Conditions for Operations with Private Individuals, and internal acts of the Bank regulating the business on accounts involved with direct channels' use, including all amendments to these by-laws during the contractual relationship between the User and the Bank.

17. CLOSING PROVISIONS

The General Conditions of Use shall come into effect on the day of their adoption by the Bank Supervisory Board, and shall be applied upon the expiry of the fifteenth day from their release on the internet portal of the Bank (http://www.unicreditbank-bl.ba).

Starting from the day of the beginning of the application of the General Conditions of Use, the General Conditions of Use of Direct Channels of UniCredit Bank a.d. Banja Luka no. NO-87/18 dated 27.04.2018 shall cease to be valid.

No. NO-127/19