DIGITAL BANKING PLATFORM

inspired by you

Available on
Web, Mobile & Tablet

Raiffeisen BANK

DIGITAL BANKING TERMS AND CONDITIONS

RAIFFEISEN BANK SHA

DATE 12.01.2017

Table of Contents

I. INTRODUCTION

These General Terms and Conditions regulate the rights, obligations and rules of using the Digital Banking platform which the Bank provides to any Company holding at least an active current account with the Bank.

Definitions:
Individual terms used in these General Terms and Conditions shall have the following meaning:

"Digital Banking" refers to the electronic banking platform offered by Raiffeisen Banks Sh.A to the Company in order to access the Account(s) via the website www.24.raiffeisen.al/Corporate and/ or mobile application, hereinafter Internet and Mobile Banking . Digital Banking includes services such as view and details of all products with the bank (Current and Saving Accounts; Loans; Deposits; Cards) and Transaction processing (transfer of funds; bill payment; state budget obligations; salary processing) and any other service that Raiffeisen Bank Sh.A may decide to provide from time to time via the Digital Banking platform. The availability/non-availability of a particular service shall be communicated to the Company/User through email, web page of Raiffeisen Bank Sh.A or in writing as may be deemed fit by the Bank.

"Internet Banking" refers to the Digital banking service offered by Raiffeisen Banks Sh.a to the Company in order to access the Account(s)/ Products via the Web Internet.

"Mobile Banking service" refers to the service which Raiffeisen Bank Sh.a provides, in order to enable the Company to access his Account(s) via the Mobile Banking Application.

"24/7" means the service's availability twenty-four hours a day, seven days a week[1].

"Company" means any legal entity or an entrepreneur legally registered for conducting business activity, who has at least an active operating current account opened with the Raiffeisen Bank Sh.A.

"User" refers to an individual duly recognized by Raiffiesen Bank Sh.A who is authorized from the Company's Legal Representative/s through the Application Form, to access and use Digital Banking.

"Working Day" means days between and including Monday to Friday and do not include public holidays and weekends.

"User's Equipment" means all such compatible equipment and devices, software (including any necessary App downloads), communication lines (including public communication lines) and mobile devices which are able to use Google Android and Apple's iOS operating systems, used and required by the User to properly access any of the Services.

"Compatible Equipment" shall be considered all equipment the Customer is obliged to have on its computers and mobiles which will be using Digital Banking services a licensed, regularly configured operative system. Supported operative system and browsers are as follows: IE 9+, Chrome, Mozilla, Opera, Microsoft edge. The mobile application is supported on Android version 4.4+ and iOS version 8+.

"Security Elements" means SMS OTP, Mobile Cronto or Hardware Cronto.

1 1. For Urgent Value Date and Forex Cut of Times please refer to Annex 1 – Treasury Cut off Time

"PIN Code" – combination of at least 4 numbers defined during activation of mobile application or hardware device. PIN is used for authentication to unlock mobile application and security elements and authorization of mobile only payments.

"SMS OTP" (One Time Password) means one-time secret number issued to the User in the registered mobile number, which the Bank presumes that is accessed and known exclusively by him. SMS OTP will be used to identify the User and will be part of the sign up process and activation of the other security elements, mobile Cronto and Hardware Cronto.

Mobile Cronto – authentication application integrated with Digital Banking mobile app. After activation this component of mobile app can be used to authenticate users and to authorize transactions.
Hardware Cronto – out of bound authentication device, where user can activate dedicated security license. After activation this device is used to authenticate users and to authorize transactions.
Daily Limits - means the maximum payment volume ordered within one day. This is the company limit only for the Digital Banking channel

II. GENERAL PROVISIONS

2.1 Digital Banking services can be used by any Company that holds an active current account opened with the Raiffeisen Bank Sh.A.

2.2 In order to achieve approval by the Bank for usage Digital Banking services, the Company's legal representative/s must fill out and sign the following documents:

- Application Form for using Digital Banking services (hereinafter: The Request) which must be filled with i) all the relevant data related to the account number/s, ii) the way of signing for specific account (single, jointly signing) and iii) mark all relevant fields necessary for usage of that specific service.

- The List of individual User's rights accompanied with the type of security elements chosen to be issued for any of them respectively.

Moreover, the Company is obliged to submit, along with specified documentation herein, valid personal IDs of the individual Users to whom access will be given in Digital Banking Platform.

2.3 The User may start accessing Digital Banking only after the Bank has notified the latter on this purpose. For the sake of clarity, the Bank must firstly approve the Request and create the User on the bank systems by issuing also the respective security elements in this regard.

2.4 By signing the Application Form, the Company that the Bank has provided him with any and all information regarding the Digital Banking service, and that also any and all documents pertaining to the Agreement were made available to him. The signature on the Application form represents the Company's confirmation that all the rights and obligations arising from the made Agreement are understood and agreed by him.

2.5 The Company understands that must have available sufficient funds in its account/s in the BANK to cover all its liabilities towards the Bank and the transfer orders executed by any User through the Digital Banking Service. Should the funds on the account/s are not sufficient to cover the payment order the BANK shall reject the execution of the transaction. The rejected transaction shall receive status "Not Successful", which shall be considered as a notice from the BANK that the payment shall not be executed.

2.6 Based on the List of Individual Users, the Bank shall issue security elements for each User with defined privileges for the specified accounts. Company may request changes in the defined privileges for an individual user under specified accounts or defining privileges for additional accounts. The request for change or modification, signed by the authorized/Legal representative may be submitted in person or by post.

2.6.1 Notwithstanding above, for extraordinary cases the Bank may accept such request scanned via e-mail with the sole condition that the original copy must be submitted within 5 working days pursuant to the predictions of article 2.6 above. Should the Company fail to perform such obligation within the defined timeline, the Bank has the right to immediately block the Service. For the sake of clarity, in any change of modification via e-mail as a scanned copy, risk of possible abuse of the specified changes as well as material consequences shall be borne by the Company.

2.7 When contracting the Digital Banking service, the Bank offers a particular range of services which the Company accepts by signing the Application Form. The services are listed and described in the Application form for the use of the respective Digital Banking service and/or Security Device. The Bank retains the right to amend the range and content of services at any time without any specific approval by the Company. Any and all ads and amendments to the already agreed Digital Banking services or, the list of the new launched services, will be published by the Bank in its official website and in the Platform as well. The Company is aware and fully agrees that the usage of these new services may be performed by it or its Users only by endorsing the respective Application form amendment.

2.8 By signing these General Terms and Conditions, the Company gives its unconditional consent and irrevocable authorization to the Bank that, under its sole discretion due to improvements, safety measures or changes in the current legislation, revoke or change the daily limits for the payment orders placed with the Bank to be executed through the Digital Banking service. The Bank will priory notify at least 15 days in advance the Company on any implementation, revoking or changing the daily limits set by the Bank by delivering a notification via the Digital Banking service to which the respective daily limit refers, if such service supports such particular notification manner, otherwise the Company will be notified through e-mail in its chosen address in the Application form.

2.8.1 Moreover, the Company agrees that The BANK has the right to impose restrictions for realization of operations through Digital Banking on the basis of the requirements of the applicable legislation, the internal regulations of the BANK, the present General conditions and the maintaining of proper safety of its systems.

2.9 For the purpose of identifying the Company and/or the User of the Device, increasing service quality, blockade of the Device or a service for security and other reasons, the Bank retains the right to record legally any and all Online Help conversation referring to the Digital Banking service chat, telephone call or other type of communication. By signing the Application, the Company explicitly confirm that they are familiar with and consent to the fact that the Bank may record any and all outgoing and incoming telephone calls, and that, in the case of a potential dispute, the respective recorded conversations can be used as evidence.

2.10 For the given privileges for the Exchange Office service, the individual User whose rights are granted to execute transactions with preferential conversion rate within Company's own accounts, may perform this action without any additional company user confirmation.
The User shall have 60 seconds to confirm or reject the preferential rate given by the Bank. By confirming the offered exchange rate, the single User will give the authorization that the chosen account will be debited for the specified currency amount equivalent of the bought foreign currency or vice versa. For the sake of clarity, this action may be performed only by a single User, regardless the chosen limit for that specific account.

2.11 Transactions executed through Digital Banking service in favor of third parties' accounts (excluding payments predicted in article 2.12 below) will require authorization elements like mobile Cronto or

Hardware Cronto and the Bank shall not perform payment orders through Digital Banking in case the User fails to carry out the authorization requirements.

2.12 Transfer towards Own Accounts in Raiffeisen Bank Sh.A, Business Credit Card Payments and Preferential Rate(Exchange Office) are authorized without any security elements.

2.13 During the execution of any payment (salaries included) through Digital Banking, the Bank commits to credit the account / IBAN given by the User itself and in such regard, the Bank does not bear any responsibility or be held liable to crosscheck the inputted data if they fit with the beneficiary name pre-filled by the User during the payment authorization.

2.14 The Bank shall not be held liable for any damage resulting from or in connection with errors in transmission, technical problems of any kind and nature, line interruption, interference with facilities established and managed by third parties, including but not limited mobile operators, private network suppliers. The risk of the defects in the User's own hardware or software and the misuse of the identification features shall be borne solely by the Company.

2.15 The Company fully understands and gives its irrevocable consent that the Bank shall not be held liable for any damage or loss caused to the Company which come as a result of violation of any of these Terms and Conditions by any of the authorized Company's Users.

III. SECURITY ELEMENTS RULES

3.1 Pursuant to the written authorization given by the Legal Representative(s) of the Company in the Application Form, the BANK shall provide to the Digital Banking User a soft integrated in mobile application and/or a hardware device for identification and authorization – token /hereinafter called Mobile and Hardware Cronto device. These security elements will be accessed by PIN that should be defined by user himself/herself. The Mobile and Hardware Cronto are used for authorization of transactions, in particular signing and sending payment orders by the Digital Banking Users on behalf of the Company.

3.2 Any and all potential monetary, reputational or goodwill loss derived as a result of fraudulent and/or negligence misconduct actions performed by Users during the conduct of Digital Banking service, shall be borne solely and exclusively by the Company. In this respect, the Company understands that this responsibility shall not be limited even in those cases when the security elements are made known to third parties due to the fact that the Company and/or its authorized Users fail to safeguard the given security elements as per the below instructions:

a) The Bank advises that selecting easily guessed combinations passwords and/or PIN and/or personal information such as telephone numbers, date of birth, or a recognizable part of Client's name or initials should be avoided.
b) Passwords and/or PIN used for the Service should not be used for accessing other services (for example, connection to the internet or accessing other websites, or Pin for cards).
c) User must take reasonable steps to keep the security elements safe and the password/PIN secret and to access the Service in a secure manner to prevent fraud or abuse. In particular, the Company (and any other authorized user) should take all reasonable precautions including, but not necessarily limited to:
i) not allowing anyone else to use the password and PIN or disclosing their passwords to anyone including, Bank's staff, the Police or other authorities. The Bank's staff will never ask for User's password. If in doubt, Company/User should immediately contact the Bank's address given on Article

3.4 below;

ii) never write down the password and PIN on the security the security elements on anything usually kept with or near it;

iii) should not write down or record the password without disguising it;

iv) not disclose their personal information such as information on their identity card or passport, addresses, or bank accounts, to any persons failing to prove their identities or any doubtful websites;

v) Do not let security elements unattended. For SMS OTP and Mobile Cronto the device used are respectively mobile phone where is active the mobile number declared in bank and smart phone where mobile app is activated, and for Hardware Cronto is the dedicated hardware provided from bank.

3.3 It is a Company's duty and obligation to properly and individually instruct any of the authorized Users with the minimal security elements as predicted on Article 3.2 above. In this context, the Company shall be assured priory giving access to the Digital Platform that any of the Users has taken the proper training in such regard. The Company acknowledges that via the issuance of the Cronto to the User, the Bank shall be relieved by any responsibility in regard with its usage in terms of disposal of the Digital Banking.
It shall remain a joint responsibility of the Company and the User the misuse of the Digital Platform for all actions and/or consequences performed in the Digital Banking platform afterwards.

3.4 In case of loss of the authentications elements or if there are grounds for suspicion that an unauthorized person may have acquired knowledge thereof, the Company shall inform the Bank immediately by calling the Bank Call Center in the phone number +355 42 381 381 and in the electronic mail digitalbanking.support@raiffeisen.al by e-mail so the Bank can arrange for the blockage of the authentications elements and as a result, the access to the Digital Banking Platform by this respective User whose credentials are lost. The Company shall be entitled to demand the blocking of access by written request at any time, even without naming any reasons thereof. Access will be blocked automatically in case of repeated attempts at gaining access by the use of incorrect authentication elements.

3.5 The Cronto hardware performance is guaranteed by the Bank for a period up to 18 months starting from its receipt to the User. Should this device show defects within the aforesaid period excluding any physical, mechanical, weather or damages arisen from improper use, the Company shall file a written request to the Bank for a new device. Should the Bank find this request as compliant with the guarantee policy, it is obliged to submit to the User a new Cronto device.

3.6 In the event of the token being lost /stolen/uncovered damages on point 3.5, the BANK shall make a new Hardware Cronto available to the Company against payment of an actual commission charges according to the current Tariff of the BANK.

3.7 After multiple (3 time) consecutive incorrect password entry, Digital Banking will be blocked for 24 hours and the User can wait for the account to be auto unlocked or in case the unlock is needed before this time the user will be obliged to initiate once again the sign up process. Before starting the new sign up process the Company may fulfil a reactivation request in order to authorize the user to re-signup log in in Digital Banking. The request for re activation signed by the authorized/Legal representative may be submitted in person or by post. For extraordinary cases please refer to pint 2.6.1.

3.7.1 After multiple (3 time) consecutive incorrect PIN/OTP/Response Code entry, the user security elements will be locked for a predefine time. After this time, shown on the message that will appear in the application, the security element will be automatically unlocked. If the user's security elements are locked two consecutive times the Company may fulfil a reactivation request in order to authorize the user to re access security elements of log in Digital Banking. The request for re activation of security elements signed by the authorized/Legal representative may be submitted in person or by post. For extraordinary cases please refer to pint 2.6.1.

3.8 The User shall provide the Bank with all relevant data and information of any changes that affect or are likely to affect the usage/functionality of the Cronto.

3.9 In case of problems or Errors with Digital Banking, the User must send the Session ID to digitalbanking.support@raiffeisen.al

3.10 The Company is responsible for the mobile number that have declare in the Bank. This number will be used for sending SMS OTP which are used as security elements for enrollment and credentials changes(username/password).

3.11 The user accepts the security elements (SMS OTP, Mobile Cronto, Hardware Cronto) as an exclusive proof of its identity during the use of the services of Digital Banking service, without the right of denying it in the future. By using the security element, the possibility of false representation is disabled, which means that a reliable authenticity of the User is provided.

IV. PAYMENT ORDERS

4.1 Upon completion of authentication/authorization procedure (username/Password/ PIN/OTP/ Cronto Image) and the fulfillment of mandatory data of a payment order, the Bank will display a message with the status of the payment (Processed /Pending treasury approval /Not Successful / Reject)

4.2 Payment orders will be executed automatically as per cut off time ANNEX 1.

4.3 For any cancellation or amendment request regarding an executed payment, the Company must send an official request to the address corporatesupport@raiffeisen.al with payment data that is required to be canceled / amended. The bank, based on its internal procedures, will conduct the respective verifications and confirmations regarding the Company's request and will confirm for the outcome of the process.

4.4 Any order placed with the Bank through the Digital Banking Platform by a person using the above-mentioned authentications elements that legitimize/authenticate him as a User to this platform, shall be deemed as a valid order placed in the name and on behalf of the Company, irrespectively to the legal relationship between that individual and the Company and irrespectively of whether the placing of the order was effected with or without the knowledge or an authorization by the Company.

4.5 The Bank reserves the right to interrupt or cancel Digital Banking service and to block the ongoing placed order payments in case when the Company's accounts are inactive, blocked or has outstanding due debts towards the Bank.

4.6 The User may place orders in foreign currency abroad Albania only in compliance with Bank of Albania Regulation on Foreign Exchange Activity and the Company must provide to the Bank the justifying documents within 5 working days from the date of the payment execution by attaching the documents in Digital Banking. In case of failure on providing the justifying documents within the predefined period, the Bank shall not execute any succeeding payment order/s performed on behalf of the Company, despite the User who will place this/these order/s.

4.7 Capital Transfers outside the territory of the Republic of Albania are not allowed to be performed through the Digital Banking service.

V. OBLIGATIONS AND RESPONSIBILITIES OF THE BANK

5.1 The Bank retains the right to reject a Company's Application for contracting Digital Banking service or remove the service at any time without supplying any explanation for such decision if the Company does not comply bank or regulatory requirements.

5.2 The Bank shall execute received payment orders in accordance with the applicable legal regulations.

5.3 Payment or transfer orders and other electronic documents sent by the User via Digital Banking shall be considered authorized and authenticated documents.

5.4 The Bank is not responsible for any disturbances or interruptions in the telecommunication network as well as for the consequent unavailability of Digital Banking service which it may cause. The Bank reserves the right to conduct regular maintenance of Digital Banking service. The client will be notified in advance for the bank maintenance schedule. During the regular maintenance, Digital Banking will be unavailable to the User.

VI. FEES

6.1 The Company shall pay the fees for the use of Digital Banking services and for Cronto elements, in accordance with the current Bank 's Terms and Conditions.

6.2 The contracted Digital Banking service is activated only after the agreed Service's fees are duly paid by the Company. Should the Company fail to ensure available funds in the predefined account to cover the agreed Service's fees, the Bank has the right to put that account in a debit balance for the due fee's amount.

6.3 Notwithstanding the above prediction, in case of a Company's failure to pay the agreed fees, the Bank reserves the right to unilaterally terminate the Agreement.

VII. JURISDICTION

7.1 These Terms and Conditions shall be governed by the Albanian law. Unless otherwise agreed upon herein, the General Terms and Conditions of Raiffeisen Bank Sh.A. shall apply. For any dispute arising in connection with this Agreement the parties will try to amicably solve it and if this will not be achievable, the Tirana's District Court shall be competent to finally resolve the dispute.

Anex 1

<table>
<tr><th colspan="3">Preferential Rate</th></tr>
<tr><th>Cut off Time</th><th>Limit</th><th>Confirmation Timer</th></tr>
<tr><td rowspan="2">Before 16:30 PM CET</td><td>> EUR 1.000 (eqv. in other currency)</td><td rowspan="2">After Bank Confirmation, the client must confirm the rate in 60 sec</td></tr>
<tr><td>< EUR 1.000 (eqv. in other currency)</td></tr>
<tr><td>After 16:30 PM CET</td><td colspan="2">N/A</td></tr>
<tr><td colspan="3">Note: This payment can be executed only in Exchange Office widget</td></tr>
</table>

Anex 1

Normal Value Date – Cut off Time											
Payment	Type	Cut off Time	Limits for CCY (eqv. in EUR)								Execution Date	Credit Value Date
			ALL	USD	EUR	GBP	CHF	CAD	AUD	JPY		
Within the bank	Same currency	Working Hours	24/7								D	D
		Non-Working hours										
	Different currency	Working Hours	24/7								D	D
		Non-Working hours	< EUR 10.000				< EUR 2.000				D	D
			> EUR 10.000				> EUR 2.000				N/A	N/A
Within the bank	Same currency	Working Hours	24/7								D	D+2
		Non-Working hours	24/7								D	D+3
	Different currency	Working Hours	24/7								D	D+2
		Non-Working hours	< EUR 10.000				< EUR 2.000				D	D+3
			> EUR 10.000				> EUR 2.000				N/A	N/A

Note: Cut off = 09:00 AM -16.30 PM, after cut off=16:31 PM -08:59 AM, CET)

Anex 1

Urgent Value Date – Cut off Time												
Payment	Type	Cut off Time	Limits for CCY (eqv in EUR)								Execution Date	Credit Value Date
			ALL	USD	EUR	GBP	CHF	CAD	AUD	JPY		
Within the bank	Same currency	Working Hours	24/7								D	D
		Non-Working hours	24/7								D	D
	Different currency	Working Hours	24/7								D	D
		Non-Working hours	< EUR 10.000				< EUR 2.000				D	D
			> EUR 10.000				> EUR 2.000				N/A	N/A
Outside the Bank	Same currency	Working Hours	< 30 mio	< 0.5 mio	< 0.5 mio	< 0.1 mio	< 0.1 mio	< 0.1 mio	D + 1	D+1	D	D*
			> 30 mio	> 0.5 mio	> 0.5 mio	> 0.1 mio	> 0.1 mio	> 0.1 mio	D + 1	D+1	D	as per Treasury confirmation
		Non-Working hours	N/A									
	Different currency	Working Hours	< 30 mio	< 0.1 mio	< 0.2 mio	< 0.05 mio	< 0.02 mio	< 0.03 mio	D + 1	D+1	D	D*
			> 30 mio	> 0.1 mio	> 0.2 mio	> 0.05 mio	> 0.02 mio	> 0.03 mio	D + 1	D+1	D	as per Treasury confirmation
		Non-Working hours	N/A									

*as per Currency cut off time

inspired by you