

## GENERAL CONDITIONS FOR THE PERFORMANCE OF BANKING OPERATIONS FOR NATURAL PERSONS

**CONTENT: 1. Introduction; 2. General principles; 3. General conditions applicable to the accounts; 4. Provisions regarding the payment operations; 5. Contractual provisions relating to the issue and use of the Card; 6. Special services offered by the Bank through the Call Center of Raiffeisen Bank; 7. Terms and conditions for the Direct Debit Service; 8. Final provisions; 9. Client's Statements and Parties' Signatures.**

### 1. INTRODUCTION

#### 1.1. Introductory Provisions

**1.1.1.** These General Conditions for the Performance of Banking Operations (hereinafter referred to as "GBC") set the general legal framework for the development of the contractual relationship between Raiffeisen Bank S.A. (hereinafter referred to as the "Bank") and each of its Clients, natural persons.

**1.1.2.** The legal relations between the Bank and the Client will be governed by these GBC which, together with the provisions stipulated in each of the contractual documents particular to each type of banking product or service, concluded between the Bank and the Client, will represent the contract between the parties. These GBC complete the contractual documents particular to the banking products/services, unless otherwise provided in the content of the latter.

**1.1.3.** In case there are matters that are not expressly regulated, the enactments in force, the regulations of the National Bank of Romania, the Bank's norms, as well as the domestic and international banking practices and usages will be applied to the legal relationships between the Bank and the Client.

**1.1.4.** The Bank will enter into contractual relations with the persons who accept these GBC.

Any new Client will receive a copy of the GBC, in force on the date of the Client's registration in the Bank's records.

By signing any other request in the form provided by the Bank or any other specific Agreement, the Client accepts that, during such contractual relations with the Bank, it will observe the GBC in force at that moment, with possible amendments which may be made by the Bank subject to these GBC.

#### 1.2. Conflicts

**1.2.1.** In case of conflicts between the express provisions in any Agreement or document signed between the Client and the Bank and the general provisions included in these GBC, the express provisions in the Specific Agreements or documents shall prevail.

**1.2.2.** The Client accepts both the Romanian version of the GBC as well as the English version thereof, in case of any conflict or discrepancies between the English and the Romanian versions, the Romanian version shall prevail.

#### 1.3. Interpretation

**1.3.1.** Any reference to the Bank in this document will be understood as including any of its territorial units (field office, representative office, agency, branch) also.

**1.3.2.** Any reference made to the Client herein also includes the category of Co-debtor and/or Guarantor, if applicable as per the Specific Agreements.

**1.3.3.** Any reference to the Client – natural person herein will be deemed to have been made also to any of its successors.

**1.3.4.** The reference to the Borrower in the Specific Agreements will be deemed as having been made to the Client, as it is defined in these GBC.

**1.3.5.** The plural will include the singular and vice versa anywhere in these GBC and/or in any Specific Agreement, unless otherwise required by the context.

**1.3.6.** The reference to "significant adverse effects" or to "significant alteration" will be construed as reflecting the qualified opinion of the Bank.

**1.3.7.** The reference to any Specific Agreement/Warranty Agreement/any other convention concluded between the Client and the Bank or to any legal provision will include any amendment, reiteration or reinforcement thereof.

**1.3.8.** The headings of these GBC and/or in any Specific Agreement/Warranty Agreement/specific contractual documentation have been introduced only to facilitate the references and they do not affect the interpretation of the provisions of such contractual documents.

#### **1.4. Independent clauses**

In case any provision from these GBC and/or from any of the Specific Agreements executed between the Bank and the Client is or becomes at any point void, invalid or unenforceable according to the applicable law, then the lawfulness, the validity and the enforceability of such provision within the limit approved by the law, as well as of the other provisions of GBC, will not be affected or damaged thereby. The parties will use their best endeavours to draft those documents and/or amendments which would lead to the same legal and/or economic result which was taken into account on the date the GBC were executed.

#### **1.5. Definitions.**

For the purposes of these GBCs, the terms and expressions below have the following meanings:

**ATM (Automated Teller Machine)/MFM (Multi-Functional Machine)** - electronic terminals of the Bank or other payment service providers that allow Customers, who hold a Card, to perform transactions or other banking operations (e.g. cash withdrawals, balance inquiries, bill payments, cash deposits - only at MFM, etc.);  
**Strict Client authentication** = authentication based on the use of two or more items included in the category of knowledge held (something that only the Client knows, for example PIN, password), possession (something that only the Client owns, for example the card) and inheritance (something that represents the Client, for example, fingerprint, facial recognition) that are independent, and compromising one element does not lead to compromising the reliability of the other elements and which are designed in such a way as to protect the confidentiality of authentication data;

**The Bank** = Raiffeisen Bank SA, as Credit Institution, payment service provider and/or provider of any other service and/or banking product, in accordance with the activity object authorized under the law;

**Card** = payment instrument issued by the Bank, through which the Client has access to its own money availabilities from the Current Account and/or to a credit line, in order to carry out Card Transactions; the Card can be issued either on physical or virtual medium, the available card types are listed on the Bank's website [raiffeisen.ro](http://raiffeisen.ro), in the Debit Cards/Shopping Cards section.

**Card Transaction** - is the payment transaction (deposit, withdrawal, transfer or collection of funds) made by/on behalf of the Card User by means of the Card, including the Card registered in the eWallet or any mobile device with payment function;

**Currency conversion fee** - the fee charged by the Bank, expressed as a percentage of the foreign exchange rate applied by the Visa card organization in accordance with the provisions of chapter 5.4 of these GTC and which is added to this exchange rate; the amount of this fee can be found on the Bank's website in the Foreign Exchange Rate - Card Transactions section;

**Client** = natural person, resident or non-resident in Romania, who opens a contractual business relationship with the Bank that includes but is not limited to opening and operating Accounts and/or providing/supply by the Bank with/of various banking services/products;

**Beneficiary Client** = the Client who benefits from the funds that are the subject of a Payment Operation;

**Paying Client** = the Client who instructs a payment order;

**Internal identification code/CIF Key/Client code** - unique code assigned by the Bank to persons registered in its database, needed for the unique identification of persons in a relationship with the Bank;

**Account** = bank account in which the client's cash availability and/or as the case may be, the amounts made available by the Bank at its disposal are highlighted; any reference to "Account" includes a reference to "credit card account" unless expressly provided otherwise;

**Payment account** = Account used mainly for the performance of the payment operations;

**Payments account accessible online** = current account owned by the Client that can be accessed through an online interface, such as the online mobile banking application made available by the Bank;

**Specific Agreement** = the contract that regulates the supply/provision of any product/service provided by the Bank and any other accessory or related legal relationships with it. Specific documents with standard and/or negotiated content make up the Agreement, which reflect the agreement between the Bank and the Client, as well as, but not limited to, requests approved by the Bank, offers accepted by the Customer, Credit agreements, guarantee contract, conventions, communications, notifications, forms and/or any other documents related to the specific Contract, accepted by the Bank;

**“The Bank's foreign exchange rate”** - the exchange rate used by the Bank for foreign exchange or payment transactions carried out on the account, expressed in a currency other than that of the payer's account, respectively of the payee's account, calculated as follows: **(i)** in the case of foreign exchange conversions of the foreign currency/lei type, the Bank's buying rate shall be used for the currency in which the amount transferred to the payee's account is expressed, respectively the Bank's selling rate shall be used for the currency in which the amount transferred by the payer is expressed; **(ii)** in the case of foreign currency/ foreign currency conversions, the ratio of the exchange rate obtained from the Bank's foreign currency/lei buying rate for the currency in which the amount transferred by the payer with an account at another bank is expressed and the Bank's foreign currency/lei selling rate for the currency in which the amount credited to the beneficiary's account is expressed shall be used, i.e. the rate obtained from the ratio between the Bank's exchange rate for the currency in which the amount transferred to the beneficiary with an account at another bank is expressed and the Bank's exchange rate for the currency debited from the payer's account.

In the case of payment transactions authorized by means of Cards, the exchange rates expressly mentioned in this document under the provisions on the use of Cards shall apply.

The currencies for which the Bank offers currency conversion services are published on the Bank's website [www.raiffeisen.ro](http://www.raiffeisen.ro).

**Exchange rate for card transactions** = the internal exchange rate of the Bank for foreign exchange, for sale, respectively the purchase of the reference currency, used to perform Card Transactions displayed in its territorial units or on the Bank's website [www.raiffeisen.ro](http://www.raiffeisen.ro);

**Debit card agreement** = the specific contract that regulates the contractual relations between the Bank and the Card User, derived from the use of the debit card attached to a current account, consisting of the clauses provided in these GBC and the clauses found in the specific documentation for issuing and maintaining the Debit Card;

**Current account agreement** = Specific contract regulating the contractual relations between the Bank and the current account holder, consisting of the clauses provided in these GBC and the clauses found in the specific documentation of opening and maintaining the current account, in the forms used to define and update the personal data of the Client and for the appointment. and revocation of the Power of Attorney on the account;

**Contract regarding the direct debit service** = the specific contract that regulates the contractual relations between the Bank and the Payer, derived from the activation of the Direct Debit Service, consisting of the clauses provided in these GBC and the clauses found in the forms for issuing, modifying and denouncing the Direct Debit Mandates;

**FATCA (The Foreign Account Tax Compliance Act)** = is a legislative package issued in the United States of America, which can be viewed at <http://www.treasury.gov/resource-center/tax-policy/treaties/Pages/FATCA.aspx>, enacted March 18, 2010 and which entered into force on July 1, 2014, which requires the taxpayers of the United States of America ("USA"), including those living or operating outside the United States, to report direct or indirect holdings of assets outside the US. The same reporting requirement is provided for credit institutions, which hold assets on behalf of US taxpayers.

**Effective date** = the reference date used by the Bank to calculate the interest generated by the execution of a Payment Operation;

**Transaction Posting Date on the Account** - or Transaction Date is the date on which the Card Transaction amount is debited from the Account and transferred to the payee via the card scheme;

**CRS (Common Reporting Standard)** = represents the global standard for automatic exchange of financial information between countries. The income from investments (including interest, dividends, capital gains, etc.) held by taxpayers in the accounts of financial institutions from the countries participating in the global exchange of financial information are targeted. The global standard for the exchange of financial information and the multilateral agreement for the automatic exchange of information were initiated by the OECD (Economic Organization for Cooperation and Development) and the European Commission. The standard has three

directions: the information to be reported, the reporting institutions and the accounts that are the subject of the report. Romania provides the legal framework by transposing the European provisions in the Fiscal Procedure Code, which entered into force starting January 1, 2016.

**Signatory** = the person with full exercise capacity, authorized by the Client, by means of the special forms provided by the Bank or by the notarial power of attorney, to have access on behalf and on behalf of the Client to an Account opened on its behalf, acting within the limits provided in the Specific Agreements;

**Payment instrument** = any personalized device and/or any set of procedures agreed between the Client and the Bank under the contractual conditions agreed with the Bank, used by the Client to initiate a payment order such as the Card, mobile banking service etc.;

**Principal** = the person authorized by the Client through the power of attorney to represent it in relation with the Bank for the conclusion and/or execution of an agreement. The power of attorney for representation must be authenticated by a notary public in Romania or at a Romanian consulate; in the case of the proxies issued to a notary from abroad, the proxy will be apostilized or over-legalized, as the case may be, and a legalized translation of it will be presented, if written in a foreign language;

**The moment of receipt of the Payment Order** = the day on which the Payment Order, transmitted directly by the Payer or indirectly by or through a Payee, is deemed to have come into the Bank's possession, depending on the Cut-Off Time; as a rule, for Payment Orders received on Business Days up to the Cut-off Time, the time of receipt is the day of receipt by the Bank, and for Payment Orders received after the Cut-off Time, the time of receipt is the next Business Day; if the Payment Order is received on a non-business day, the time of receipt is considered the next Business Day, regardless of the payment instrument or the method used to transmit the Order. A Payment Order whose execution has been refused by the Bank shall be deemed not to have been received;

Exception: **(i)** direct debit banking services, which allow the Payee to initiate Payment Transactions, as well as those of the scheduled payment order type, whereby the Payor Customer orders payments with a pre-determined frequency, in the case of which the Time of Receipt is the day agreed by the Bank and the Customer in the specific Contract; **(ii)** other services or types of payments offered by the Bank which allow the receipt and execution of Payment Orders outside the time limits mentioned above;

**Payment operation** = action initiated by the Paying Client or another person on his behalf and on behalf of him or the payee in order to deposit, transfer or withdraw funds, regardless of any subsequent obligations between the payer and the payee; The payment operation may be occasional;

**BEN commissioning option** = means of commissioning the execution of the payment operations according to which the beneficiary of the payment supports all the related commissions;

**OUR commissioning option** = means of commissioning the execution of the payment operations according to which the payer supports all the commissions related to the execution of the payment operation;

**SHA commissioning option** = means of commissioning the execution of the payment operation according to which the Paying Client supports the commissions received by the payment service provider of the payer, and the Client receiving the payment supports the commissions received by the payment service provider of the beneficiary. The possible commissions of the correspondent/intermediary banks are due/received according to the European/international practices and of the SWIFT standard;

**Deadline for receiving the Payment Order** = time set by the Bank to take possession of the Payment Order, according to which the moment of receiving it is established. The time limit may be different depending on the type of Payment Operation/Payment Instrument and it is communicated to the Client as the case may be, by posting in specially arranged places in the Bank's units and/or on the website [www.raiffeisen.ro](http://www.raiffeisen.ro) and/or in the specific Agreement/information applications related to certain services provided by the Bank;

**Payment order** = the instruction given by the payer or the beneficiary of the payment to the Bank, as a payment service provider, requesting the execution of a Payment Operation;

**Static password** = security element included in the category of knowledge (something that only the Card User knows) which the Card User sets at the first Card Transaction made on the internet (within e-commerce);

**Security password in the relationship with the Bank** = identification procedure, used during the Customer's interaction with the Bank's Call Center telephone service, which fully proves the identity of the Customer/Card User and his/her will regarding the content of these calls. The identification procedure consists of requesting security elements and information known only to the Bank and the Client/Card User, and the telephone calls

will be recorded in order to provide evidence in this respect. Obtaining correct answers to the questions of the virtual operator / Bank operator is equivalent to validating the identity of the caller / person called by the Bank. If the telephone number from which the call was initiated in the Call Center does not correspond to the telephone number registered in the Bank's database as belonging to the Client/Card User, the Bank reserves the right not to proceed with the caller's request until the telephone number is updated by going through the specific procedures for updating the contact details of these persons;

**PIN**= is a unique identification code generated by the Bank for each Card, in order to identify or secure certain Payment Operations performed through the Card such as ATM / MFM transactions, some transactions through EPOS at merchants or at bank branches.;

**Low-Value Card Transactions** = represents the payment operation whose individual value is less or at most equal to the limit established by the international organizations of cards, Visa/Mastercard, however, which cannot exceed EUR 50 or an equivalent amount for EPOS transactions, respectively EUR 30 for internet transactions (e-commerce); the limit value is set by international card organizations, depending on the country and can be changed at any time by these entities; the limit value applicable on the territory of Romania is mentioned for information in the specific Contracts of debit card and credit card and is permanently displayed in the units and on the Bank's website, any update of the limit value will be displayed on the website;

**Electronic wallet** = payment computer application installed on one or more mobile devices such as smart phone (smartphone), tablet, smart watch (smartwatch) etc. which allows card registration and Card transactions, using a mobile device with payment function, under the conditions established in application by its supplier and/or the Bank;

**Provider of information services regarding accounts** = service provider authorized by a competent authority from Romania and/or from the EU/EEA member states, which has the right to provide information services regarding payment accounts in the territory of Romania, through which the Client can request information regarding its payment accounts, accessible online, held at the Bank;

**Payment initiation service provider** = a payment service provider authorized by a competent authority in Romania and/or in the EU/EEA member states that is entitled to offer payment initiation services on the territory of Romania, through which the Customer can initiate payment orders on his/her online accessible payment accounts opened with the Bank;

**Qualified trust service provider** = a legal person providing one or more qualified trust services and granted qualified status by the supervisory body. Qualified Trusted Service means an electronic service which fulfils the applicable conditions laid down in Regulation (EU) No 910/2014, which is typically provided for remuneration, and which consists of: (i) the creation, verification and validation of electronic signatures, electronic seals or electronic timestamps, registered electronic distribution services and certificates related to those services; or (ii) the creation, verification and validation of certificates for the authentication of a website; or (iii) the maintenance of electronic signatures, seals or certificates related to those services;

**Interest rate** = annual percentage of determined/determinable interest, according to Specific Agreements and/or Specific Interest Lists, used as the basis of calculation for interest;

**Reference rate** = the interest rate that comes from a public source that can be verified by both the Client and the Bank;

**Legal representative** = the person representing the Client in the contractual relations with the Bank, within the limits of the applicable legislation and/or of the provisions of the competent authorities/courts (for example: parent, guardian, curator, other categories provided by law); In order to demonstrate the quality of the Legal Representative, documents provided by the law must be submitted (for example, a court decision on minor entrustment, the decision to establish guardianship and the appointment of the legal representative etc.);

**Electronic signature** - electronic signature accepted by the Bank in relationship with Customers, which may be a qualified electronic signature, advanced electronic signature, or simple electronic signature, as provided for by the legislation in force;

**Biometric signature** - an electronic signature created using a specialized electronic device (e.g., an electronic tablet) that records the biometric data of the holographic signature executed by the person concerned using a specialized device (electronic pen);

**Call Center Service** = telephone service made available by the Bank to customers which can be accessed at \*2000 (normal rate number, callable from any mobile network in Romania) and +40213063002 (normal rate number, callable from any network, from Romania and from abroad), available 24/7; the Call Center service uses public telephone lines, which may not ensure an adequate level of information protection, by calling this service the Client assuming the risks of disclosing data/information derived from this situation;

**Specimen signature** = signature of the Client to be used in relation with the Bank for valid instructions;

**Contactless technology** = technology that, using radio waves, allows Card transactions to be carried out by simply approaching the Card or mobile device with payment function, an EPOS terminal or other terminals compatible with this technology;

**Terminal** = device compatible with the Card and/or with the mobile device with a payment function, through which Card transactions are initiated and authorized. The following devices are Terminals: ATM (Automated Teller Machine), EPOS (Electronic Point of Sale), Imprinter, MFM (Multi Functional Machine) and any other device with similar functionalities;

**Credit Transfer** = payment service by which the payment account of the payment beneficiary is credited as a result of a payment operation or a series of payment operations carried out from the payment account of the payer by the payment service provider who holds the payment account of the payer, based on an instruction given by the payer; In the present GBC by the references to "payment operation"/"payment" is understood to include a reference to "credit transfer";

**Card transaction** = is the payment operation performed by the Card User through the Card, including the Card registered in the Electronic Wallet or any mobile device with payment function;

**Card recurring transaction** = is a series of transaction made as a result of the authorization given by the Card User directly to the trader, on its website or by any other means, in order to debit the card account at regular intervals, for the payment of goods and services according to the authorization granted to the trader

**Card users** are any of the following:

a) Main Card user ("Main user") = is the natural person with full or restricted exercise capacity, holder of a current account or a credit card, who asks the Bank to issue a Card attached to the account;

b) Additional Card User ("Extra User") - is the natural person with full exercise capacity who has access to the amounts from the main user's account, through additional cards (one Card for each user), based on the agreement expressed by the main Card User, either in the documents made available by the Bank, or in the telephone calls carried out through the Call Center Service, or within the mobile banking applications available to it;

**Working day** = day when the Bank carries out activity that allows it to execute payment operations; In relation to the Bank, the Saturdays, Sundays, public holidays, any other days considered non-working by the Corresponding Banks/External settlement systems in the case of payment transactions carried out through them, as well as the days on them are considered to be non-working days, which the Bank declares to be non-working days, in this situation the Clients will be informed in a timely manner by displaying the corresponding messages inside the Bank's units and on its website.

## 1.6. Notions and provisions regarding the fight against money laundering and terrorist financing and application of the International Sanctions

### 1.6.1 Definitions

**Embargo** = An act of authority by which a state takes interdiction measures against the importation of goods from a certain country, either against the export of goods to another country, as a sanction for non-observance of rules of international law or as a means of political pressure.

**Digital wallet provider** - means an entity that provides services for the secure storage of private cryptographic keys on behalf of its customers for the holding, storage and transfer of virtual currency; (This term shall be used throughout these GBCs and any specific Contract with the meaning defined under Law no.129/2019 *on preventing and combating money laundering and terrorist financing, as well as for amending and supplementing certain regulatory acts*; in the event of any legal changes to this definition, they are of direct application, without the need to amend this document);

**Virtual Currency** - means a digital representation of value that is not issued or guaranteed by a central bank or public authority, is not necessarily linked to a legally established currency and does not have the legal status of currency or money, but is accepted by natural or legal persons as a means of exchange and can be transferred,

stored and traded electronically; (this term shall be used within these GBC and any specific Contract with the meaning defined under Law no.129 /2019 *on preventing and combating money laundering and terrorist financing, as well as for amending and supplementing certain regulatory acts*; in the event of any legal changes to this definition, they shall be of direct application, without the need to amend this document);

**International sanctions** = sanctions, restrictions and obligations in relation to the governments of some states, non-state entities or natural or legal persons, adopted by the Security Council of the United Nations, the European Union, the United States of America, international organizations or by unilateral decisions of Romania or of other states that Romania decides to implement for the purpose of preserving international peace and security, preventing and combating terrorism, ensuring enforcement of human rights and fundamental freedoms, development and consolidation of democracy and rule of law and accomplishing other goals, in compliance with the objectives of the international community, with the international law and with the European Union law. International sanctions are aimed, in particular, at freezing funds and economic resources, commercial restrictions, restrictions on operations with dual-use products and technologies and military products, travel restrictions, transport and communications restrictions, diplomatic sanctions or in the technical-scientific, cultural areas or sports.

**Authorities with responsibilities in the field of issuing and managing the International Sanctions** - mean either of:

- a) United Nations Organization (UNO);
- b) European Union (EU);
- c) Government of the United States of America;
- d) Congress of the United States of America;
- e) State Secretariat for Economic Affairs of Switzerland;
- f) Any Member State of the European Union, including, in any case, but not limited to, the Republic of Austria;
- g) United Kingdom of Great Britain and Northern Ireland
- h) the respective governmental institutions and agencies of any of the foregoing states, including but not limited to the Office of Foreign Assets Control (OFAC), the Secretary of the Treasury of the United States of America, the Department of State of the United States of America, Office of Financial Sanctions Implementation in United Kingdom (OFSI), part of Her Majesty's Treasury in United Kingdom or any (other) relevant government institution or regulatory authority or agency that administers economic or International sanctions (each as amended, supplemented or replaced from time to time).

**List of Sanctions** = “Specially Designated Nationals and Blocked Persons List” maintained by the Office of Foreign Assets Control, a governmental agency of the United States of America) and the “Consolidated List of Financial Sanctions Targets in the UK maintained by The Office of Financial Sanctions Implementation in the UK (OFSI's Consolidated List) and any other list of persons sanctioned by the United States Department of State, as published in the federal Registry or any other list managed by any Authority responsible for issuing and/or managing International Sanctions, each of them as amended, supplemented or replaced from time to time;

**List of reportable jurisdictions** – list of countries with which automatic exchange of information is carried out, maintained by ANAF;

**Sanctions** = economic or financial sanctions or restrictions (such as described) or embargoes imposed, managed or applied, from time to time, by either of the Authorities responsible for issuing and managing International Sanctions;

**US Sanctions** = economic or financial sanctions or embargoes imposed, managed or applied from time to time by the United States Congress, by the Government of the United States of America, by the United States Department of the Treasury or by the Office of Foreign Assets Control - OFAC, (each authority as amended, supplemented or replaced from time to time);

**Designated persons/entities** = state governments, non-state entities or persons subject to International Sanctions.

**Restricted party** = any of the following:

- a) person/entity designated or person/entity owned/controlled by a designated person/entity (insofar as it is within the scope of the requirements regarding the ownership or control structure of the relevant sanctions) or a person/entity acting on behalf of a designated persons/entities; or

- b) person/entity located or organized in accordance with the legislation of a country or territory that is subject to International Sanctions at country or territory level or which is owned/controlled by such person/entity (insofar as it is within the scope of application of the requirements regarding the ownership or control structure of the relevant sanctions) or a person/entity acting on behalf of such person/entity; or
- c) person/entity that is the subject of the relevant International Sanctions in another way.

**Asset** - any technology or product of economic value or intended to satisfy a specific purpose, tangible or intangible, which belongs to or is owned or controlled by designated persons or entities or which is subject to sectoral sanctions; funds and economic resources are assimilated to the definition of assets;

**Funds** - financial resources and benefits of any kind, including, but not limited to: cash, checks, cash receivables, bills of exchange, payment orders, and other payment instruments; deposits with financial institutions or other entities, account balances, receivables, and debt securities; publicly and privately traded securities and debt instruments, including securities and shares, certificates representing securities, bonds, promissory notes, guarantees, unsecured bonds, and derivative contracts; interest, dividends, or other income or profits derived from or generated by assets; loans, counterclaims, guarantees, performance bonds or other financial commitments, including insurance and reinsurance; letters of credit, bills of lading, contracts of sale; shares in funds or economic resources and documents evidencing their ownership;

**Freezing of funds** - any action intended to prevent the movement, transfer, modification, use, access, or transactions with funds, likely to result in a change in their volume, value, location, ownership, possession, nature, or destination, or any other change that would allow the use of funds, including portfolio management; Economic resources - assets of any kind, tangible or intangible, movable or immovable, which are not funds but can be used to obtain funds, goods, or services;

**Freezing of economic resources** - preventing the use of economic resources to obtain funds, goods, or services in any way, including by sale, lease, or mortgage;

#### **1.6.2 Notions from the legislation on preventing and combating money laundering and terrorism financing.**

**1.6.2.1** In accordance with the provisions of the aforementioned legislation, publicly exposed persons are natural persons who exercise or have exercised important public functions.

By important public functions we mean:

- a) heads of state, heads of government, ministers and deputy ministers or secretaries of state;
- b) members of Parliament or similar central legislative bodies;
- c) members of the governing bodies of political parties;
- d) members of the supreme courts, constitutional courts or other high-level courts whose decisions can be challenged only through extraordinary means of appeal;
- e) members of the governing bodies of the courts of accounts or members of the governing bodies of the boards of central banks;
- f) ambassadors, persons in charge with business and senior officers in the armed forces;
- g) members of the boards of directors and of the supervisory boards and the persons holding management positions of the autonomous administrations, of the companies, with majority state capital and of the national companies;
- h) directors, deputy directors and members of the board of directors or members of the governing bodies of an international organization.

**1.6.2.2** None of the categories referred to in the preceding paragraph includes persons holding intermediate or lower positions.

**1.6.2.3** Family members of the publicly exposed person are, for the purposes of this law:

- a) the spouse of the publicly exposed person or his/her partner with whom he or she is in similar relationships to those between spouses;
- b) the children and their spouses or their spouses, the persons with whom the children are in relationships similar to those of the spouses;
- c) the parents.

**1.6.2.4** People known as close associates of publicly exposed persons are:

a) the natural persons known as the real beneficiaries of a legal person, of an entity without legal personality or of a legal construction similar to them together with any of the persons mentioned in point 1.6.2.1 or as having any other close business relationship with such the person;

b) the natural persons who are the only real beneficiaries of a legal person, of an entity without legal personality or of a legal construction similar to them, known as being established for the de facto benefit of one of the persons mentioned in par. section 1.6.2.1.

Without prejudice to the application, based on a risk assessment, of the additional measures of knowing the client, after the expiration of a period of one year from the date when the person ceased to hold an important public function in the sense of point 1.6.2.1., the reporting entities no longer consider that person to be publicly exposed.

**1.6.2.5** The notion of ultimate beneficial owner (“UBO”) shall mean any natural person who finally holds or controls the client and/or the natural person on whose behalf a transaction, an operation or an activity is carried out.

## 2. GENERAL PRINCIPLES

### 2.1 Provisions regarding personal data protection

Relevant **DEFINITIONS** in the context of personal data protection

**Personal data** = any information regarding an identified or identifiable natural person; <sup>[1]</sup>an identifiable natural person is a person who can be identified, directly or indirectly, especially by reference to an identification element, such as a name, identification number, location data, an online identifier, or to one or more specific elements, its own physical, physiological, genetic, psychological, economic, cultural or social identity;

**Personal data processing** = any operation or set of operations performed on personal data or on personal data sets, with or without the use of automated means, such as: collecting, recording, organizing, structuring, storing, adapting or modifying, extracting, consulting, use, disclosure to third parties by transmission, dissemination or in any other way, joining or combining, blocking/restricting, deleting or destroying;

**Right to information** = the right of the data subject to be informed about the processing of his personal data, including the identity and contact details of the operator and of the Data Protection Officer, the purposes for which the data processing is done, the categories of personal data concerned, the recipients or categories of data recipients, the existence of the rights provided by the legislation regarding the protection of personal data for the data subject and the conditions under which they can be exercised;

**The right of access to data** = the right of the data subject to obtain from the data operator (such as the Bank and the Credit Bureau), the confirmation that the personal data they are targeting are processed or not and, if so, access to the respective data and to relevant information regarding the processing of personal data;

**The right to rectification** = the right of the data subject to obtain the rectification of inaccurate data concerning him, as well as the completion of incomplete data;

**The right to delete data ("the right to be forgotten")** = the right of the data subject to obtain, as long as the conditions stipulated by the law are fulfilled, the deletion of the personal data concerning that person;

**The right to restrict the processing** = the right of the data subject to obtain, as long as the conditions provided by the law are met, marking of personal data stored, with the purpose of limiting their further processing;

**The right to data portability** = the right of the data subject to receive, the personal data concerning him and which he provided to the operator (such as the Bank) in a structured way, commonly used and - an easy-to-read format, as well as the right for these data to be transmitted by the operator (such as the Bank) to another data operator, insofar as the conditions provided by law are fulfilled);

**The right to opposition** = the right of the data subject to oppose at any time, for well-founded and legitimate reasons related to his particular situation, that the personal data that aims to be the object of processing, insofar as the conditions stipulated by the law are fulfilled. When the processing of personal data concerning him has the purpose of direct marketing, the data subject has the right at any time to oppose the processing of his data for this purpose;

**The right not to be subjected to an individual decision** = the right of the data subject to request and obtain the withdrawal, cancellation or reassessment of any decision based exclusively on processing by automatic

means (including the creation of profiles) that produces legal effects on the data subject or it affects it similarly to a significant extent;

**The right to go to court or before the National Supervisory Authority for Personal Data Processing** = the right of the data subject to complain to the National Supervisory Authority for the Processing of Personal Data, respectively to address the justice for the defence of any rights guaranteed by the applicable legislation in the field of protection of personal data, which have been violated.

**Raiffeisen Group** = the group consisting of the following entities: Raiffeisen Bank S.A., Raiffeisen Broker de Asigurare - Reasigurare S.R.L., Raiffesien Leasing Financiar IFN S.A., Aedificium Banca pentru Locuinte S.A., SAI Raiffeisen Asset Management S.A., Raiffeisen Bank International AG and the entities that are part of the group Raiffeisen Bank International AG. More information is available at <https://www.raiffeisen.ro/despre-noi/cine-suntem/raiffeisen-bank-international/>.

**2.1.1.** In order to provide the banking services assumed under these GBCs, the Bank processes personal data, in accordance with the legal provisions applicable in the field of personal data protection, respectively the General Regulation on Data Protection no. 679/2016 and the subsequent legislation.

**2.1.2.** The personal data that are processed by the Bank belong to the following categories of data subjects: the Client (even after the termination of the contractual relationship) including the holder of the request for liquidation of the bearer savings books/password-protected bearer savings books, the legal or conventional representatives of the Client, the Power of Attorney / Users of the Client, Co-debtors, Guarantors, Real beneficiaries, members their families (including the Client's husband/wife) in the context of the Client's request for the suspension of monthly instalment payments under the circumstances of COVID-19 pandemic, other Client's family members (parents and children who live or household with the Client) – as the case may be as well as any other natural persons whose data could be provided to the Bank by the Client or which could be processed in the context of the relationship between the Bank and the Client (together, generically referred to as „Data subjects”). In the context of fulfilling the legal obligations incumbent on Raiffeisen Bank as a Secondary Insurance Intermediary - Affiliated Agent or for the fulfillment of all processing purposes in relation to insurance, Raiffeisen Bank processes or may process personal data regarding the following categories of Data Subjects: Insurance Applicant, spouse of the Applicant/Client, Client, his/her spouse, his/her legal or contractual representatives, children or other family members, as well as the life partner of the client/potential client, Co-debtors, Guarantors (if applicable, including when they have the status of Insured, owners of the property to be insured, mortgaged or not in favor of the Bank, the Beneficial Owners, as well as for their family members, depending on the type of insurance to be purchased through the Smart Mobile application and its coverage), the owners of the properties for which the Clients conclude the insurance as Contractors, the co-insureds, the insurance contractors or any other natural persons in relation to the client/potential client, whose personal data may be processed depending on the type of insurance, where applicable, including as co-insureds. These personal data are transmitted to the Bank at the beginning of the contractual relations with the Client or are disclosed to the Bank during their course. The Bank may process the personal data belonging to the Data Subjects and after the termination of the contractual relationship with the Client, in order to comply with the legal obligations incumbent on it, including the incidental obligations regarding the archiving matter.

**2.1.3.** In certain situations, in order to fulfil the processing purposes mentioned in this document, the Bank may process personal data belonging to certain categories of Data Subjects (for example, the Real Beneficiaries, the Client's husband/wife, other members of the Client's family - parents and children living or householding with the Client, the owners of the properties for which the Clients conclude the insurance as Contractors, co-insureds, insurance contractors or any other natural persons in relation to the Client/potential Client, whose personal data may be processed depending on the type of insurance concluded by the Client, etc.) , without benefiting from the practical way of directly informing these categories of persons. For example, this can happen if the Client transmits the data of the Data Subjects to the Bank. In this context, it is the Client's responsibility to inform in advance the persons concerned about the processing of their personal data and to obtain their consent regarding the processing of the data, to the extent necessary, in order to fulfil the conditions provided by the law. Also, if the Customer provides the Bank with personal data belonging to other categories of Data Subjects, the Customer is obliged to provide only accurate and up-to-date data. In this regard, the Bank may use the contact details of such categories of Data Subjects to inform the persons concerned about the processing of their personal data, if applicable. Particularly, in the event that in the context of submission of a request for suspension of the monthly

instalment payment obligation according to the Government Emergency Ordinance no. 37/2020 on granting facilities in relation to loans granted by credit institutions and non-banking financial institutions to certain categories of borrowers (“GEO 37/2020”) or at a subsequent time in the context of this request, the Client provides us with personal data of his family members (data relating to their health, social, financial, professional condition or any other relevant data in relation to them in the context of the respective request) the Client is responsible for ensuring that he informs his family members with a view to their personal data processing by the Bank, prior to the submission of their data to the Bank according to the provisions laid down herein.

**2.1.4.** The Bank processes personal data for the following purposes, as follows:

**2.1.4.1.** In order to fulfil the legal obligations, the Bank processes the personal data for: the execution and improvement of the banking services offered by taking in the Bank's information applications the data from the identity document, according to the applicable legal requirements; getting to know the client in order to prevent money laundering and combat terrorist financing and complying with the international sanctions regime, including by creating and using warning lists; perform customer identification operations in the context of the contractual relationship, according to the legal obligations; preventing and reducing the risk related to fraud and corruption and guarantee of banking secrecy including by verifying the authenticity of the presented identity document and by taking the necessary steps to identify the client; ensuring compliance with applicable legal requirements in the field of financial investment services, including providing expert advice and support to the Bank's employees in this area; checking compliance with internal regulations and local legal/regulatory requirements; transaction reporting and other statutory reporting; the receipt, assessment and management of the Client's request for the suspension of the monthly instalment payment obligation, in the context of COVID-19 pandemic; conducting internal audits and investigations; administrative-financial management; managing conflicts of interests; managing the controls performed by the authorities; preventing market abuse; fulfilling the obligations of banking supervision on the Bank and of the entities of the Raiffeisen Group and of reporting to the entities of the Raiffeisen Group or to the supervisory authorities and other internal reporting, including for the fulfillment of the legal obligations of Raiffeisen Bank International AG – entity mentioned in the definition of the Raiffeisen Group managing incidents that may occur during the execution of the contract between the Client and the Bank; data analysis for reporting to regulators, risk portfolio analysis, advanced analytics to improve the effectiveness of compliance monitoring and verification, data management through single systems across the Raiffeisen Group; use of IT systems and IT services including for the storage of data processed through applications and systems, management of complaints and notification received, both with respect to an unrelated to contracted banking products and/or services; complying with the prudential requirements applicable to credit institutions and the groups to which they belong, including requirements for fiscal due diligence; applying the tax due diligence and reporting measures provided by the legislation in force to the competent tax authorities (including ANAF), in order to achieve the automatic exchange of information (FATCA, CRS), the compliance procedures provided for in the FATCA Agreement; managing credit risk by creating profiles; assessing the eligibility for the provision of standard or personalized banking products and services (including at the granting/approval phase) from the risk perspective by analysis and creating profiles in order to evaluate the solvency, reduce the credit risk and determine the degree of indebtedness, including verification of risk criteria, calculation of payment behaviour rating/transactional rating, calculation of turnover, determination of risk class; assessing investment behaviour by creating profiles; portfolio management; liquidity management and balance sheet optimization; the provision of banking services consisting of payment transactions/involving banking transactions – (a) initiated by a Data Subject (as this notion is defined in section 2.1.2 above), as the initiator of its payment or (b) initiated to a Data Subject (as beneficiary of the payment, including the generation of a document attesting the operation of the respective operation (confirmation of the operation - if applicable, respectively statement of account); processing of payment/collection operations through SWIFT, SEP, SENT, REGIS, TARGET systems, as the case may be; conducting in good condition the transactions of processing of the banking transactions, including the management of the quality of the data related to the operations of processing of the transactions and ensuring a unitary way of completing the mentions of the payment orders in the electronic messages used in this context; providing the information regarding accounts in case of the requests made by the Data Subjects through a Provider of information services regarding the accounts; execution of the payment orders initiated by the Data Subjects through a Provider of payment

initiation services; the provision of banking services consisting in the payment of invoices to the MFMs of the Bank, through Raiffeisen Smart Mobile Service or through Post Offices; the provision of the direct debit service; setting up and managing the garnishments, providing information on garnishment amounts to enforcement bodies or authorities; the provision of the cash distribution service through the network of the Bank branches; ensuring security in the Raiffeisen premises and its branches; storage, storage (pre-archiving) and document archiving; data quality management; implementation of security measures for personal data; the transmission and reception within the Raiffeisen Group of information regarding the state of non-repayment; the transmission of information about the granted credit, specifically the individual credit risk and the situation of overdue credits (including delays in payment exceeding 30 calendar days) to the Center Credit Register within the National Bank of Romania (an independent public institution headquartered in 25 Lipscani Street, District 3, Bucharest, which represents a specialized structure in collecting, storing, and centralizing information regarding the exposure of each reporting entity—credit institution, non-bank financial institution, payment institution, etc. from Romania, towards those debtors who have benefited from credits and/or commitments whose cumulative level exceeds the reporting limit (20,000 lei), as well as information related to card frauds committed by holders), assessing the requirements and needs regarding the contracting of an insurance product and for providing consultancy to customers, according to the legislation on insurance distribution and the Norms issued by the Financial Supervisory Authority in this matter, knowing the customers in order to fulfill the legal obligations of the Bank in its capacity as Intermediary, Affiliated Agent; assessment of eligibility for the provision of insurance products. In the event that the Client submits to the Bank any information related to his disease or of one/some of his family members' COVID-19 disease, the Bank shall process this category of data exclusively for major public interest reasons, under the GEO no. 37/2020, which was adopted precisely in the major public interest for the purpose of taking actions to fight against the negative effects of COVID-19 influencing the economic situation of certain categories of debtors. In this context, art. 5 para. (3) of the Norms for implementing GEO no. 37/2020, approved under the Decision no. 270/2020 set forth under art. 5 para. (3) that the debtor should indicate in the request addressed to the creditor the reason which leads to the impossibility of fulfilling the loan payment obligations, indicating inclusively the COVID-19 disease as a possible cause.

In order to fulfil the aforementioned purposes, the Bank will, as far as necessary, be based on its legitimate interest in carrying out its object of activity and/or on the contract between the Client and the Bank.

**2.1.4.2.** In order to conclude and execute the contract between the Client and the Bank, it processes the personal data for: collecting documents and information necessary for the conclusion of contracts related to financial-banking products and services, including for carrying out a risk assessment in order to make a decision on the application for a financial-banking product or service; concluding, conducting and managing the contractual relationship with the Client, in order to provide financial-banking products and services (including online services and the functionalities and operations available through these services), including in the context of handling the Client's request for suspension of the instalment obligation in the context of the COVID-19 pandemic, as well as insurance products - for this processing purpose the Bank and the insurer involved may act as Joint Controllers (the relevant information to other situations, where the Bank and the insurer would act in a different capacity, will be provided through the flow-specific disclosure documents applicable in those situations) and including for the purpose of cashing bearer/password bearer savings books; assessing the requirements and needs regarding the contracting of an insurance product, according to the legislation on insurance distribution and the Norms issued by the Financial Supervisory Authority in its application, providing advice to the Client, carrying out and managing the contractual relationship with the Client in the name and for the insurer and/or together with the insurer, in order to provide the appropriate insurance products among the insurance products that it intermediates in as an affiliated agent; collection of insurance premiums for the insurer; ensuring the technical support and maintenance activities necessary for the development and management of the contractual relationship with the Client; registrations in the RNPM, as appropriate; providing information on accounts in the case of requests made by the Client through a Provider of information services on accounts; execution of payment orders initiated by the Customer through a Payment Initiation Service Provider; managing incidents that may occur during the execution of the contract between the Client and the Bank, by creating and drawing up warning lists, for example, in case of unauthorized discovery of an account; the optimization of financial-banking services, including by providing technical support and maintenance activities; data quality management; providing advice and information on insurance distribution; conclusion

and/or execution of insurance contracts; evaluation of the goods proposed under guarantee; monitoring all the obligations assumed by any of the entities in the Raiffeisen Group; debt collection/debt collection and their pre-financing activities; finding, exercising or defending some rights of the Bank in court; managing the complaints and notifications received regarding the contracted banking products and/or services; verifying compliance with internal policies and regulations.

In order to fulfil the aforementioned purposes, the Bank shall, as far as necessary, be based on its legitimate interest in carrying out its object of activity.

**2.1.4.3.** In order to fulfil the legitimate interests of the Bank, in the context of carrying out its object of activity, the Bank processes the personal data for: the obtaining and the transmission of data by accessing the Credit Bureau (Biroul de Credit) before entering and during the credit relationship that falls within the scope of the rules on the Credit Bureau - for this processing purpose, the Bank and Biroul de Credit SA act as associated operators; the provision of information regarding accounts in the case of the requests made by the Data Subject (as this notion is defined in section 2.1.2 above) through a Provider of information services regarding accounts and the execution of payment orders initiated by the Data Subject through a Provider of payment initiation services, if such activities involve the processing of data belonging to other Data Subjects besides the Bank Client; facilitating the Bank's fulfilment of its supervisory obligations vis-à-vis entities in the Raiffeisen Group; ensuring an adequate level of knowledge of the clients of the entities of the Raiffeisen Group, inclusively by transmitting personal data of common customers to the Bank and the entity of the Raiffeisen Group - Aedificium Banca pentru Locuinte S.A. - and, if applicable, of the Data Subject in relation to the respective common clients (if applicable) for the proper management by Aedificium Banca pentru Locuinte S.A. of the contractual relationship with their Clients, including for ensuring the practical possibility of Aedificium Banca pentru Locuinte S.A. to recover debts and send contractual notifications based on updated personal data, inclusively by communication of information to the entities within Raiffeisen Group, regarding prospective clients (leads) who have expressed their interest regarding one of the products of another entity within Raiffeisen Group – for this processing purpose the Bank and the relevant entity within Raiffeisen Group act as associate operators; obtaining information regarding the conduct of the insolvency procedure regarding the Data Subjects by accessing the Insolvency Procedures Bulletin; internal processes and flows optimization, including the detection of anomalies on current accounts and transactions; conducting profiles and analyses to prevent and reduce the risks of fraud by creating and using warning lists; ensuring the possibility of exercising the Bank's rights by conducting research to identify the assets owned by the Data Subjects that are in the Bank's record with outstanding amounts; selection, profiling and segmentation activities for the purpose of analysis and marketing, including for the purpose of offering the most suitable products and services, inclusively by communication of information to the insurer, with a view to supply the insurance products – for this processing purpose the Bank and the insurer concerned may act as associate operators and inclusively by communication of information to the entities within Raiffeisen Group, including for the purpose of offering the most adequate products and services or with a view to identify and assess the potential payment difficulties by determining the early warning indicators, by consulting the data provided directly by the Data Subjects, the data generated by the Bank regarding the Data Subjects and the collected data by the Bank from external sources (such as data related to the warning lists and other lists made and kept at the Bank level such as list of confiscations, litigation list; transactional data or resulting from the use of Raiffeisen Bank products and services; relationship history data with the Bank or other entities in the Raiffeisen Group; data collected from public sources and from Raiffeisen Bank's contractual partners); improvement of the banking products and services provided and of the experience of the data subjects, including by optimizing the flows and internal regulations, by optimizing the costs and budgets, by ensuring the technical support and the maintenance activities; customer segmentation; increasing the level of digitization and enhanced efficiency within the Bank, by reducing efforts, including financial efforts, to manually perform similar processes, also through the creation and implementation of advanced analytical models; the conclusion, implementation and management of execution of the agreements concluded with other clients of the Bank (legal entities) for the provision of banking services consisting in the payment of the invoices to the MFMs of the Bank, through RaiffeisenSmart Mobile Service or through the Post Offices, the provision of the direct debit service, the provision of the cash distribution service through the network of the Bank branches; designing, developing, testing and using IT systems and IT services (including storing databases in the country or abroad); advertising, simple marketing and advertising, as well as the preparation/personalisation

of offers (to the extent that the personalisation techniques do not attract the consent referred to in point 2.1.4.4. below), including the use of data obtained from the Credit Bureau in the context of the monitoring of the active credit portfolio in order to personalise such offers, including to promote the products of contractual partners through online channels such as social networks; commercial communications by means of communication not covered by direct marketing rules (e.g., by letter, telephone call made by a human operator); streamlining the process of creating and carrying out marketing campaigns/campaigns, by collecting information on how Data Subjects interact with marketing communications sent by the Bank, e.g. by e-mail and/or SMS, and by generating statistics/aggregated data/information on the effectiveness of the marketing campaigns/campaigns carried out; documenting how contracts are executed with contractual partners whose products are promoted by the Bank; statistics; managing complaints and notifications that do not concern the banking products and/or services contracted by the Data Subject; the generation of account statements for the Authorized (except the Authorized on the account), the agent of the account holder, respectively the legal representative of the minor account holder; the inclusion of non-commercial messages in the account statements; transmitting the information on account garnishments (unless prohibited by law); improving the insurance consultancy activity; managing complaints and notifications that do not concern the banking products and/or services contracted by the data subject from Raiffeisen Bank, keeping records on the intermediated insurance contracts; keeping and archiving the recordings of audio and/or audio-video interactions if the data subjects have chosen to use such communication channels made available by the Bank and have expressed their consent to make the recordings at their initiation; storing and archiving the history of conversations between the Data Subject and the Bank on the chat in the Bank's applications.

Additionally, in order to fulfill the Bank's legitimate interests, the Bank processes personal data through low-risk artificial intelligence models, including advanced machine learning, also by the training and development of these models, to enhance internal operational activities, to improve the Bank's results and reports, by automated data processing, also by automate the processing of information specific to certain documents by extracting and centralizing the information, automate the drafting and translation of documents, transcribe calls made through the call center and appropriately mark the purposes of the communication, create specific internal documents and analyses, automatically reconcile certain transactions, systematize certain analyses, and create mechanisms for the automatic extraction of certain data and information, increase the level of digitization, and reduce human intervention to obtain data/information related to the accounting and profitability of the Bank's customers. To the extent that the Bank will use high-risk models or systems, it will comply with the requirements established by Regulation (EU) No 2024/1689 of the European Parliament and of the Council of 13 June 2024 on laying down harmonized rules on artificial intelligence.

In order to prevent fraud among clients (individuals or legal entities) who make electronic payments, as well as to reduce erroneous transactions caused by incorrectly entering the beneficiary's account (IBAN format account), the Bank has implemented the Beneficiary Name Display Service (SANB ). This service involves the automatic display of the first name and the initial of the last name of the payment beneficiary (in the case of individuals), or the truncated name if the beneficiary of the payment is a legal entity, at the moment the payer enters the IBAN code in the banking applications through which electronic payments are made.

For the operation of this service, in order to fulfill the legitimate interests of the Bank and TRANSFOND, which acts for these purposes as a co-operator with the Bank and all other banks participating in SANB, the personal data of the Data Subject, namely: the initial of the last name, full first name, and IBAN code, are transferred by the Bank to Transfond, where they are stored and periodically updated until the termination of the relationship with the Bank, to be interrogated by other banks participating in SANB when the Data Subject whose data is transferred by the Bank is the beneficiary of electronic payments initiated by clients of other banks participating in SANB, at the time of completing the electronic payment order, after the payer enters the IBAN code of the account into which the payment is to be made.

At the same time, the Bank has initiated the process of implementing the payment scheme called RoPay, together with other participating banks in Romania, through which it offers the possibility to Customers to benefit from a new service, which will allow payments from Raiffeisen Smart Mobile, by using the phone number of the beneficiary of the payment instead of the IBAN of the bank account. For the use of RoPay, the phone number will represent a proxy/alias of the bank account IBAN.

In order for the payment initiation scheme to work, it is necessary for all banks participating in this system to exchange information in order to create a common database, which will be managed by Transfond. For this purpose, in the first stage, the Bank, as the participating bank, will transmit to Transfond the following personal data of the Bank's individual customers who own and have activated the Raiffeisen Smart Mobile service: telephone number, IBAN code of the account in lei associated with the use of Raiffeisen Smart Mobile, name and surname. In order to carry out this personal data processing operation, the Bank will rely on its legitimate interest to participate in RoPay and to offer and implement the SPL RoPay Service, which will allow payments to be made from Raiffeisen Smart Mobile by using the payee's phone number (as a proxy/alias) instead of the bank account IBAN.

**2.1.4.4.** Based on the consent expressed by the data subject when opening the business relationship or in other situations, as the case may be, for: the processing of contact data that the Data Subject has provided to Raiffeisen Bank S.A. and periodically updated, for marketing purposes addressed to individuals, by (i) the Bank, directly and/or through its contractual partners and/or by (ii) the Raiffeisen Group and/or by (iii) the Bank's contractual partners, as the case may be, of communications of information and/or offers on products, services and activities, which may be of interest to the Data Subject in person (regardless of his / her possible relationship with a Client legal person / entity without legal personality of the Bank), and/or other entities in the Raiffeisen Group and/or its mentioned partners, as well as by the Bank, directly or through their contractual partners and/or through other entities in the Raiffeisen Group, of marketing studies regarding the Bank's current and/or future products, services and activities and/or other entities in the Raiffeisen Group and/or its contractual partners;

- the analysis of the preferences of solvency, credit risk, the degree of indebtedness and other behavioural details needed to generate personalized offers and communications of banking products and services at the request of the data subject, including by consulting the ANAF databases, as well as any databases made available by public authorities to the extent that consent is required according to the applicable requirements;
- the processing of personal data by the Bank and/or the Raiffeisen Group, directly and/or through their contractual partners, in order to generate personalized offers and communications, based on the analysis of preferences and other aspects related to the Data Subject (such as his/her behaviour) using computerized techniques (for example, cookie files, pixels and/or other similar technologies) that involve performing an automated decision-making process (including profiling) and that can produce legal effects on the Data subject (as defined in section 2.1.2 above) or that may affect it to a significant extent.

To this end, in order to transmit personalized offers and communications as close as possible to the interests of the Data Subject, including through online channels such as social networks, the Bank and/or the Raiffeisen Group may process all or only part of the data that the Data Subject provides directly in the context of the contractual relationship with the Bank, data resulting from the use of the applications made available by to the Bank, including the online applications through which the Bank provides mobile banking services, the data provided by the Bank's contractual partners, as well as data resulting from the payment transactions registered at the level of the accounts/cards held by the Data Subject. The information techniques/algorithms used allow the Bank and/or the Raiffeisen Group to identify the data subject's preferences regarding some of the categories of products and services made available by the Bank, by the entities in the Raiffeisen Group and/or by their contractual partners. Due to the preferences thus outlined and other details that result from the behaviour in the context of the contractual relationship, the Bank and/or the Raiffeisen Group will bring to the attention of the Data Subject offers focused especially on the categories of products and services that may be of interest to it. Data processing for this purpose has the benefit of making available to the Data Subject offers as adapted to their needs and interests. Also, taking into account the fact that the Bank wants to offer personalized offers, depending on the preferences and interests expressed, the Data Subject is aware that it is possible that the offers regarding products and services for which the Data Subject has not previously expressed his interest not be brought to its notice.

Additionally, the Bank will process the personal data of Data Subjects based on their consent for undergoing the remote identification process using video means, for processing biometric data and biometric verification through the use of advanced machine learning models. This consent is freely given by the Data Subjects through

digital platforms that have such a verification stage integrated, by selecting the appropriate option on the dedicated consent capture page, after going through the specific information notice.

The Bank will collect personal data based on the consent of the data subject in order to process the biometric data, necessary for signing the documents by means of the biometric signature, in the event that the client chooses to sign the documents in relation to the Bank through this method of signing, and in the situation in which this method of signing is possible.

The Bank will process the personal data of the Data Subjects based on their expressed consent and for the recording of audio and/or audio-video interactions if the Data Subjects choose to use such communication channels made available by the Bank.

The consent expressed regarding the above processing activities can be withdrawn at any time, without affecting the legality of the processing activities performed before the withdrawal, by sending a written request, dated and signed, to the addresses of any of the Raiffeisen Bank SA units (for the complete list of units, access the page <https://www.raiffeisen.ro/retea/>) or by sending an e-mail to the Bank in in this sense, at the following e-mail address: [centrala@raiffeisen.ro](mailto:centrala@raiffeisen.ro) or [actualizaredate@raiffeisen.ro](mailto:actualizaredate@raiffeisen.ro) or through the Call Center Service, Monday - Friday: 8:00 - 22:00, Saturday: 9:00 - 17:30, calling no. telephone \* 2000 - number with regular tariff, callable from any mobile telephony network in Romania .; 004 021 306 3002 - number with regular tariff, callable from any network in Romania or abroad or via the Smart Mobile app (for Customers who have activated this service).

It is possible that after providing consultancy for the conclusion of the insurance, for the purpose of concluding or administering an insurance policy and intermediation for the Clients or the payment of insurance premiums, the Bank may take over and transmit contractual documents belonging to the insurance-reinsurance company through/on the basis of which the Data Subject may provide special categories of personal data (e.g., health data), thus carrying out a data processing activity on behalf of the insurance-reinsurance company. In these cases, the expression of the consent of the Data Subject regarding this processing activity may be expressed through the specific documents of the insurance-reinsurance company, as a personal data controller.

**2.1.4.5. Automated profiling and decision making processes:** In order to fulfil the aforementioned processing purposes, in certain situations (for example, in the context of applying the client's knowledge measures in order to prevent money laundering and to combat terrorist financing, including by creating and using warning lists, in the context of identifying and assessing the potential payment difficulties by determining the early warning indicators; in the context of risk assessment carried out with a view to making a decision on the application for a credit product, i.e. with a view to providing banking services related to credit products; in the context of fraud prevention and identification, updating flow, etc.), remote identification process using video means and the processing of biometric data), the processing of personal data by automatic means is necessary.

Such processing activities may also involve the evaluation of certain aspects regarding the Data Subjects for the purpose of analysing or predicting certain characteristics regarding them, such as their education, age, economic situation, their reliability or their behaviour (including from the perspective of transactions, i.e. gambling and/or betting activities).

Based on these processing by automatic means, decisions are made, with or without human intervention, which can lead to legal effects for the Data Subjects (for example, the refusal to provide a banking product or service) or they can affect it to a significant extent (for example, affecting the financial situation of the Data Subject, such as eligibility for a credit).

Considering that the process of electronic marketing of insurance products is done automatically, through the insurer's IT solution integrated in/with the Smart Mobile application or through the Raiffeisen Bank's Smart

Mobile application, as the case may be, the assessment of the requirements and needs of potential customers and the adequacy and adequacy of the insurance product requested by them, as well as the issuance of personalized advice/recommendations is carried out by automatic means, as a result of the technical settings made at the level of the insurer's IT solution that verifies the decision of potential customers to continue the marketing process through the IT solution for a specific product by accessing the corresponding button that represents the answer to the specific question regarding the need for the product in relation to the data entered by the Customers, on the basis of which the compliance with the eligibility criteria for granting the respective insurance product is verified.

When such decisions are made without significant human intervention (i.e. an intervention that is not likely to influence the outcome of automatic processing), data processing involves an automated decision-making process. In the case of processing activities that involve such an automated decision-making process, the Data Subject has the following rights, besides the rights mentioned in point 2.1.9 below:

- a) to obtain from the Bank human intervention regarding the automated decision-making process;
- a) to express his/her point of view regarding the automated decision-making process; and
- a) to challenge the decision taken exclusively on the basis of an automatic processing that produces legal effects or affects the data subject similarly to a significant extent.

The rights can be exercised by sending a request in this regard (on paper/in electronic format, by e-mail) to: [centrala@raiffeisen.ro](mailto:centrala@raiffeisen.ro) or by contacting the Data Protection Officer at the Bank level, at the following e-mail address: [dpo@raiffeisen.ro](mailto:dpo@raiffeisen.ro).

**2.1.4.6.** The data collected for the aforementioned purposes may also be processed for subsequent purposes, but only to the extent that these subsequent purposes are compatible with the initial purposes for which the data were collected. In this regard, the Bank will take the necessary measures to analyse the compatibility of the goals, according to the legal requirements.

- a) **2.1.5.** In order to fulfil the aforementioned processing purposes, the Bank processes: a) the personal data provided directly by the Data Subject, including in the context of accessing the Bank's products and services or using the applications provided by the Bank, the remote identification process using video means and the processing of biometric data;
- b) the data obtained from the following external sources: The Credit Bureau (if applicable), ANAF (if applicable), the National Trade Register Office, the Bulletin of Insolvency Proceedings, , the Center Credit Register, public authorities and institutions, the Register of Notaries Public, available on the website of the National Union of Notaries Public of Romania, the Register of Lawyers, available on the website of the National Union of Bar Associations of Romania, the Register of Bailiffs, available on the website of the National Union of Bailiffs, the Electronic Public Register of Authorised Auditors, available on the website of the Public Authority for Public Oversight of Statutory Audit Activities, the Registers available on the website of the Romanian College of Psychologists, the Register of Mediators, available on the website of the Mediation Council, the Romanian Order of Architects, contractual partners (such as, debt collection/debt recovery agencies, service providers), entities within Raiffeisen Group, the Bank's contractual partners (including eMAG, Vodafone and other partners with whom Raiffeisen Bank SA collaborates in order to provide co-branded credit cards), the appraiser indicated for the goods offered as collateral (if applicable), notaries public (if applicable), the Target Person's employers (if applicable), the insurance or reinsurance company (if applicable), the Client (Payer), credit institutions, public sources (namely, public registries, World Check, EUR-Lex (the official EU website on EU law) ,press, lists or documents accessible to public relating to the natural persons' insolvency), initiators of the payment operations, the bailiffs, other enforcement bodies and authorities that may institute protective measures and attachments on the accounts of the Target Persons opened with the Bank, holders of the direct debit mandates, the legal representative of the minor account holder, the co-debtor who has the quality of account statement applicant, the employer of the holder of the guarantee account

opened during the employment relationship - when he has the quality of account statement applicant, Authorized of the account that has the quality of requesting account statement, other Data Subjects (e.g. in the context of debt collection/recovery actions), Transfond, General Directorate for Persons Records (DGEP).

The following categories of personal data are collected from these external sources: name, surname, Personal Identification Number - collected from Aedificium Banca pentru Locuinte S.A. (Raiffeisen Group entity), the data indicated in the specific section regarding the payment details in the context of making payments (including the Personal Code, if such data category is provided in this context), information on insurance products, data related to convictions criminal and criminal offenses public, data on suspected fraud, data on criminal prosecution, data regarding the casefiles to which the Client or Data Subjects are a party (case number, court, parties, subject matter, stage, hearing dates, solutions, other public information relating to the casefiles), number of shares held in a company, number of instalments, card number, card expiration date, transaction data, CVV/CVC code, data on the establishment of garnishment and the status of execution files, enforcement data, data collected directly from the Customer or other Data Subject/generated by service providers in the context of debt collection/claims recovery actions, such as debt collection/claims recovery agencies [data resulting from call recording (if applicable, identity data, contact details, financial situation, reason for non-payment, voice, type of relationship with the Customer, information on payments made/products/services contracted by the Customer, issues complained of/requested), data on services provided in the context of debt collection/recovery actions (where applicable, actions taken and details thereof)].

In order to: (i) comply with the Bank's legal obligations regarding the application of standard know-your-customer measures that allow it to identify the Customer and verify its identity on the basis of documents, data or information obtained from credible, secure and independent sources, (ii) the Bank's fulfillment of KYC's procedures and prevention of money laundering and terrorist financing activities, (iii) the Bank's compliance with the legal requirements regarding the accuracy and accuracy of the data, the Bank will be able to obtain from reliable, credible, independent sources, permitted by law, personal data such as: name, surname, CNP, type, series and no. the identity document, the date of issuance of the identity document, the expiry date of the identity document, the place of birth, the issuer of the identity document, the home address, the residence address, information on the date of death and the last photo of the holder of the identity document, etc.

The categories of the personal data that the Bank processes in the Credit Bureau system are identification data of the Data Subject, data related to the credit products requested/granted by the Bank, data related to events that occur during the period of the credit type product and related data. insolvency (such as those related to restructuring/refinancing, payment, assignment of credit agreement, assignment of debt, including information relating to the suspension of the monthly instalment payment obligation in the context of COVID-19 pandemic), information regarding credit-type products to which the Visited Person has the capacity of co-debtor and/or guarantor, information on opening insolvency proceedings, the number of queries. Further details on the data processed in the Credit Bureau System will be provided through the specific information documents of the flows in which such data are used.

The categories of data processed in the Center Credit Register are the identification data of the Data Subject, information regarding the type of contracted credit, the degree of indebtedness, and affiliation with a group of debtors, as well as information related to card fraud committed by holders.

In order to carry out identification and registration operations in accordance with Article 24 of Regulation (EU) No, 910/2014 on behalf of the Qualified Trust Service Provider, the Bank processes the following categories of personal data: first name, surname, personal identification code (CNP), series and number of the identity card/other document on the basis of which the identification is made (e.g. passport, certificate of residence), as well as other information that these documents may contain (e.g. date and place of birth, citizenship), signature, contact details (e.g. telephone number, e-mail), video recordings\* of the interaction with the Bank's agents for

the purpose of verifying the identity of the Data Subject. In order to provide to the Data Subject a qualified certificate for electronic signature issued by a trusted service provider, the Data Subject must provide to the Bank an e-mail address and a mobile phone number.

For the purpose of verifying a person's identity online, in the process of establishing the identity of the Data Subject, the Bank uses a remote identification method utilizing video means and the processing of biometric data. This allows the Bank to fulfill its legal obligations related to the implementation of customer due diligence measures and to prevent potential fraud attempts. The remote identification of data subjects is carried out by the Bank through digital platforms that are connected with the application of the authorized person of the Bank, through which personal data will be processed for the Data Subject to undergo the process of remote identification and perform checks to prevent potential fraud, on behalf of the Bank, for the following purposes: (i) verifying the identity document and automatically reading and extracting data through optical character recognition (OCR); (ii) biometric verification of the data subject (through the photo from the ID and the image from the video recording) and processing biometric data, using advanced machine learning models for biometric processing and verification; (iii) verifying the device from which the capture of the original identity document and the video recording are made; (iv) assigning a unique biometric numeric identifier to the face from the identity document and the video recording and verifying facial similarity; (v) other such checks. For these purposes, the Bank processes the following categories of personal data: photograph of the identity document, information extracted from the identity document and its incorporated security elements, video recordings, biometric data, metadata related to the images and the device from which the photographs and recordings were made, IP address, device properties, data about the camera and microphone on the device.

In the relationship with Raiffeisen Bank, the data subject has the possibility to sign some documents by means of a biometric signature, using the tools provided by the Bank, namely an electronic tablet and an electronic pen.

Thus, in order to generate a biometric signature, the following processing activities will be carried out:

- identification and capture at the level of the document of the action of the data subject, of signing through the tools provided by the Bank (Apple Pencil pen and Apple iPad tablet);
- through the use of specialized software, the raw data recorded by the signature pad is converted into biometric data;
- the biometric data will be encrypted during the biometric signature, at the level of the document signed by the data subject, so that the validity of the document signed by the data subject through the biometric signature is ensured.

On this occasion, the Bank will process the following personal data:

- raw data: the position of the pen on the axes (x,y), the writing angle, and the pressure applied with the pen on the tablet screen;
- data converted through specialized software: (i) temporal data (rhythm) – speed and acceleration; (ii) pressure; (iii) graphic data (the seedbed itself); (iv) angle; and (v) the difference in angle.

The data that the Bank generates based on the data provided directly or collected from external sources, respectively: customer identification code, trading data, information resulting from the non-conformities reported by any person, card number, card type, customer type, IBAN card number, PIN, card expiration date, card blocking reasons, CVV / CVC code, types of accounts held at the Bank, risk cost at customer level; the period for which the account statement is generated, where applicable, the initial and final balance, turnover, interest accrued on the statement date, maturity date, total principal repayments, total current interest and penalty repayments, days overdue, amount overdue, overdue management data, including segmentations in the context of debt collection/recovery actions, data resulting from marketing campaigns/actions.

Refusal to provide personal data may result in the impossibility of providing banking services and/or meeting the Bank's other processing purposes.

Some personal data collected by the Bank may have a special regime according to the applicable legislation, context in which it is necessary to provide additional guarantees for their processing. For example, the processing of personal data relating to criminal convictions and offenses or related security measures is allowed either under the control of a public authority or when processing is authorized by law with the establishment of appropriate borders for the rights and freedoms of the data subjects. In the case of processing such data with special regime, the Bank provides the additional guarantees provided by the applicable legislation in the field of data protection.

In the context of joining SANB, the Bank will interrogate the database belonging to TRANSFOND at the time its Clients complete electronic payment orders and will display to the Clients in the electronic payment order, after entering the IBAN code of the beneficiary's account: the full first name, the initial of the beneficiary's last name, or the truncated name of the legal entity, as additional elements for identifying the payment beneficiary that the Payer can verify before authorizing the transaction.

In the context of joining the RoPay Payment Scheme and implementing SPL RoPay, the Bank will query the SPL RoPay database managed by Transfond at the time of initiating payments by its Customers using the phone number. After filling in the payee's phone number, the Bank will display to the Customer, in the Raiffeisen Smart Mobile application, the details associated with the alias used, respectively the name and surname of the payee, as well as the IBAN code of the associated bank account, thus allowing the Payer to verify the correctness of the data related to the payment instruction, before authorizing the transaction, in order to prevent any errors and ensure that the payment reaches the correct beneficiary. Customers can be payers and/or beneficiaries of payments made through the SPL RoPay service.

**2.1.6. In order to fulfil the processing purposes, the Bank will disclose or may disclose the personal data to the following categories of recipients:** Data Subjects, legal or conventional representatives of the data subject, the debtors of the mortgaged claims (if applicable), the Bank's representatives, the appraiser indicated for the assets proposed as collateral (if applicable), notary publics (if applicable), entities of the Raiffeisen Group, the Chamber of Commerce and Industry of Romania - in the context of the registrations in the RNPM (if applicable), FNGCIMM (if applicable), Bank representatives, other natural or legal persons who process personal data on behalf of the Bank, entities of the Raiffeisen Group, contractual partners of the Bank and of the entities of the Raiffeisen Group, authorized by the Bank regarding the processing of personal data, associated operators of the Bank regarding the processing of personal data, the judicial authority, central public authorities, including ANAF (including for the FATCA CRS reports made by ANAF to the tax authorities of the partner jurisdictions), the National Bank of Romania, the Center Credit Register and the Financial Supervisory Authority, the General Directorate for the Evidence of Persons, authorities with attributions in the field of preventing and combating money laundering and terrorist financing, implementation of international sanctions, local public authorities, authorities/bodies with attributions in criminal matters, banking institutions in the context of payments initiated by the Bank Client, the beneficiary of the payment initiated by the Bank Client, TRANSFOND, the National Office of the Trade Register, Accounting information service providers, Payment initiation service providers, international organizations, service providers and goods, credit bureaus, insurance and reinsurance companies, professional organizations, market research organizations, qualified trusted service providers, debt collection/liability recovery agents, bailiffs, other enforcement bodies and authorities that may institute protective measures and attachments on the accounts of the Data Subject opened with the Bank, bank institutions participating in the Interbank Convention on direct debit, in the event of direct debit mandates of interbank type; the representatives of the National Company Romanian Post Office in the context of cash collection service through Post Offices; providers /social networks providers who may have the quality of controllers, joint controllers or processor in relation with the Bank, insurance companies for which

the Bank may act as an intermediary/affiliated agent, the Insurance Pool Against Natural Disasters (PAID), associated operators of the Bank or persons empowered by the Bank.

**2.1.7.** In order to achieve the aforementioned processing purposes, the Bank will process the personal data during necessary to fulfil the purposes of the processing, such as for the duration of the course of the banking services, as well as later, when there is a legitimate business need to do so (for example, to provide the requested information or to we respect the legal, fiscal or accounting obligations). It is possible that, following the fulfilment of the legal filing deadlines, the Bank will order the anonymization of the data, lacking such personal character and to continue processing the anonymous data for statistical purposes.

**2.1.8.** Currently, in order to achieve the above-mentioned goals, it is possible for the Bank to transfer certain categories of personal data outside Romania, to EU/EEA countries: Austria, Great Britain, Slovakia, Greece, Hungary, Germany, Ireland, as well as outside the EU/EEA, to the UK, United States of America, Kosovo. For transfers outside the EU/EEA, the Bank will establish the transfer of personal data based on standard contractual clauses adopted at the level of the European Commission or on other guarantees recognized by law.

It is possible that during the course of the activity, the aforementioned transfer states will change. You can get an updated list with the states where the personal data is transferred by accessing the Policy on the protection of personal data and confidentiality, available at <https://www.raiffeisen.ro/despre-noi/politica-de-confidentialitate/> or by sending a request to [centrala@raiffeisen.ro](mailto:centrala@raiffeisen.ro) or contacting the Data Protection Officer at the Bank level, at the following e-mail address: [dpo@raiffeisen.ro](mailto:dpo@raiffeisen.ro).

To obtain a copy of the transfer guarantees implemented by the Bank, please send a request in this regard (on paper/in electronic format, by e-mail) to: [centrala@raiffeisen.ro](mailto:centrala@raiffeisen.ro) or contact the Data Protection Officer at the Bank level, at the following e-mail address: [dpo@raiffeisen.ro](mailto:dpo@raiffeisen.ro).

**2.1.9.** The data subjects benefit from the following rights in the context of the processing of personal data: the right to information, the right to access data, the right to rectification, the right to delete data ("the right to be forgotten"), the right to restrict the processing, the right to portability data, the right to the opposition, the right not to be subject to an automatic individual decision, and the right to address the National Supervisory Authority for the Processing of Personal Data or the competent courts, to the extent that the data subject considers it necessary.

**2.1.10.** It is possible that, following the request for deletion of the data, the Bank will anonymize these data (lacking such personal character) and continue in these conditions the processing for statistical purposes.

**2.1.11.** For additional information about the processing activities carried out by Raiffeisen Bank SA, as well as about your rights in this context, please file a written application to any of the units of the Bank (for a full list of such units, please access the page <https://www.raiffeisen.ro/retea/>) or by an email to the Bank in this respect, to: [centrala@raiffeisen.ro](mailto:centrala@raiffeisen.ro).

Similarly, you may also the Data Protection Officer of Raiffeisen Bank SA, at the following email address: [dpo@raiffeisen.ro](mailto:dpo@raiffeisen.ro).

Updated information about the processing activities carried out by the Bank is available accessing the Personal Data and Confidentiality Policy available at the link <https://www.raiffeisen.ro/despre-noi/politica-de-confidentialitate/>. The information regarding the processing of personal data of the Data Subject in the context of the different products and / or services of the Bank is provided through the information documents specific to those products and / or services that were or will be made available to the Data Subject.

## 2.2 Confidentiality

**2.2.1.** The Bank and the Client shall submit all due diligence to maintain the confidentiality of the information obtained from each other in the course of the Bank-Client relationship, however, in compliance with the provisions of any law or order of a competent authority that allow or request disclosure.

**2.2.2.** The Client authorizes the Bank to process, transfer and communicate any information regarding the Client to and between the branches, agencies, work points, representatives of the Bank, companies affiliated with the Bank and agents and third partners of the Bank, for confidential use, in connection with the provision of any service to the Client (including for external payments made through a third party), as well as for the purpose of data processing, analysis, recovery of the Bank's debts, obtaining financing/warranties, transfer of the Bank's debts, as well as for statistical purposes. Any such third party may in the same way use, process and transfer in

any way the data and information regarding the Client received from the Bank within the framework of the authorization granted by the Client through this document.

**2.2.3.** The Bank will keep confidentiality and will not disclose, publish or otherwise disclose information regarding the Clients' accounts, the transactions registered therein, the contractual relations between the Bank and the Clients, without their consent.

**2.2.4.** The confidentiality clause will not apply if:

- a) the information is requested by a competent authority in a judicial procedure;
- b) the Client authorizes the Bank to disclose the information;
- c) in any other situation provided by law (i.e. providing information at the request of the corresponding financial institutions).

**2.2.5.** The Client hereby expressly consents to refusing to invoke any restrictions imposed on the Bank by the legislation in force regarding banking secrecy, for the Bank to present within the relations with third parties involved in the organizational and decision-making processes of the Bank, any information and data regarding Client or its accounts, necessary for these processes and that will not affect the Client or his business in any way. By third parties, we mean, but are not limited to, any Romanian or foreign companies that are part of the group of companies of which the Bank belongs to, specialized consultants approved by the Bank, intermediaries for certain businesses, financiers, etc. The Bank will enter into contractual relations only with the third parties involved who in turn are obliged to maintain the confidentiality of the information thus obtained.

**2.2.6.** In order to comply with the legal provisions on preventing and combating money laundering and terrorist financing, International sanctions, as well as preventing and combating fraud, the Bank may take, in its relations with the Client, the measures provided for in paragraph 3.1.4 of the GBC and any other measures it deems necessary in accordance with the legislation in force.

**2.2.7.** Raiffeisen Bank SA enforces FATCA requirements and has registered on the US Internal Revenue Service (IRS) site with the Reporting Financial Institution model IGA1 status, receiving Global Intermediate Identification Number (GIIN) 28CWN4.00008.ME.642. Accordingly, the Bank will identify US taxpayers and report to A.N.A.F. information on relevant persons and on accounts opened with the Bank by them, respectively on those accounts in which the direct or indirect holdings of financial assets by relevant persons are highlighted through the application of FATCA requirements.

**2.2.8.** Raiffeisen Bank SA applies the requirements of the CRS and, consequently, the Bank will identify the relevant CRS taxpayers and will report information on the relevant persons and on the accounts opened at the Bank by them, respectively on those accounts in which the direct or indirect holdings of financial assets by the relevant persons through the implementation of CRS requirements are highlighted.

**2.2.9.** The Client undertakes to correctly indicate the CIF key (the Internal Identification Code as defined in these GBC) whenever this code is requested by the Bank through various forms used by it in its relationship with the clients and holds the Bank harmless against any misunderstanding/damages generated by the erroneous communication of the Internal identification Code by the holder of the Current Account/Legal Representative/Client's proxy.

### **2.3. Interest. Taxes, Commissions, Other costs.**

**2.3.1.** For the products and services offered, the Bank charges to its Customers taxes, commissions, fees and, as the case may be, it receives or pays interest at the standard values contained in the specific lists, except in the situations where other specific levels are stipulated in the Specific Contracts. The specific lists can be consulted by the Customer at any of the Bank's units or by accessing [www.raiffeisen.ro](http://www.raiffeisen.ro) or [www.carddecredit.ro](http://www.carddecredit.ro).

**2.3.2.** The Bank will inform the Client about the standard conditions of fees, commissions, expenses and interest rates of the Bank in force at the time of requesting an offer regarding the products/services, as the case may be, when concluding a specific Contract.

**2.3.3.** Any interest is calculated daily on the amounts recorded in the debtor balance, as the case may be, the credit balance of the Account (current/deposit/savings/credit), based on the formula:  $D = C \cdot R_d \cdot n / N$ , where:

**D** - calculated interest;

**C** - the capital on which interest is calculated which can be the amount from the current account, the deposit capital or the credit balance;

**R<sub>d</sub>** – interest rate

**n** - the number of days in the month (which can be conventionally determined by the parties through the specific Contracts, as the actual number of days of the month for which the interest is calculated or 30);

**N** - The number of days in the year (which can be conventionally determined by the parties through the specific Contracts, as the actual number of days of the year, 360 or 365).

2.3.4. The interest rate may have a fixed and/or variable value that changes depending on (a) verifiable reference indices (such as the Reference Rate) provided in the Specific Agreements or (b) the legislative changes that require such changes. In the case of savings and term deposit accounts, the interest rate and the method of calculating the applicable interest are specified in the Specific Agreement.

### **3. GENERAL CONDITIONS APPLICABLE TO THE ACCOUNTS**

#### **3.1 General rules regarding the opening and operation of Accounts**

**3.1.1.** The accounts opened on behalf of the Client at the Bank will be governed by the terms and conditions contained in the specific Contract concluded between the Bank and the Client and by the general rules established by these GBC, as far as they are applicable.

**3.1.2.** The Bank will be able, without being obliged to do so, to open on behalf of the Clients, through its operating units and through the mobile banking service under certain conditions, Accounts (such as current accounts, savings accounts, deposit accounts, credit card accounts), as a result of their request and in accordance with the internal procedures issued by the Bank for this purpose.

**3.1.3.** The Client shall submit to the Bank, upon transmission by the Bank of any application, request or instruction or upon the Bank's simple request, any information and documents that the Bank considers necessary for the opening and operation of the Accounts, for the justification of the requested operations or for the periodic fulfilment by the Bank of the obligations established by law and/or the Bank's rules and policies. The Client undertakes to provide the Bank, at the Bank's request, any additional information, documents or statements in order to establish the purpose and/or economic rationale of the transactions, the source and/or destination of the funds withdrawn/ deposited in cash and/or the source of the funds that are the subject of the transactions, regardless of the payment channel/instrument/service through which they were initiated, to determine the source of funds invested (initially) in Virtual Coins and the financial circuit of Virtual Coins (both purchases and collections of Virtual Coins) or other information necessary in the process of knowing the clientele, updating data for the fulfilment by the Bank of the obligations established by law, by the Bank's internal rules and/or by International/US Sanctions, including information on tax residence and tax identification number.

**3.1.4. (1)** In order to comply with the Bank's customer acceptance and KYC policies and the legal provisions on preventing and combating money laundering and terrorist financing, the International/US Sanctions and the legal provisions on preventing and combating fraud, the Bank may apply one or more of the measures provided for in paragraph. (2), in any of the following situations:

- a) the Customer fails to comply with any of the obligations in clause 3.1.3;
- b) the Bank does not receive the requested information/documents/declarations or if it receives information that is incomplete, insufficient, not in conformity with reality or that cannot justify the respective Payment Transaction/Account opening.
- c) the Bank has suspicions or reasonable grounds for suspicion as to the reality/validity of the statements, documents and information provided by the Client.
- d) The Bank has reasonable suspicion or reasonable grounds for suspicion of money laundering, terrorist financing, fraud, violation of International/US Sanctions/illegal activities under applicable criminal law and/or other applicable regulations or such suspicions have been communicated to the Bank by other banks or authorities;
- e) the Bank has received trading restrictions on the Client's accounts from the competent authorities.
- f) The Bank has received requests for return of funds from originator/correspondent banks on the grounds of suspected fraud, money laundering, terrorist financing or non-compliance with International/US Sanctions.
- g) The client is a Designated Person or Restricted Party.
- h) The Client does not provide supporting documents regarding the source of funds invested in Virtual Currencies.

i) The Customer is transacting in relation to Virtual Currencies with Virtual Currency and fiat currency exchange service providers and/or Digital Wallet Providers are unauthorized/unregistered or are authorized in countries designated by the European Union as high-risk third countries and/or non-cooperative jurisdictions for tax purposes.

j) The customer conducts transactions with payment service providers in countries designated by the European Union as high-risk third countries and/or non-cooperative jurisdictions for tax purposes

k) the Customer and/or Payment transaction does not fit the risk profile established by the Bank in its internal rules.

(2) The Bank may immediately take one or more of the following measures:

(i) to refuse the Customer to contract an Account or products/services/payment instruments.

(ii) refuse to carry out Payment Transactions on the Account.

(iii) to limit the Payment Transactions that the Client may perform on his Accounts (e.g. limiting collections, cash payments, Card transactions /mobile banking services, etc.) with prior notification to the Client and specifying the term from which these limitations will apply;

(iv) to block the Account, the Card and/or mobile banking service and/or applications/payment instruments attached to the Accounts/Cards.

(v) unilaterally terminate the Contract related to the current Account or any Specific Contract related to services/products attached to the Account.

(vi) not to initiate or terminate the entire business relationship with the Customer.

**3.1.5.** If the Client is represented by a Trustee at the conclusion of the specific Account Agreement, the Client will be able to dispose of the funds in the Account only after the Signing Specimen has been deposited with the Bank.

**3.1.6.** For the accounts opened on non-working days, the date of opening the Account will be the next working day, the interest rates in force on the opening date will be applied to it.

**3.1.7.** If, under the conditions and in accordance with the law or the internal regulations of the Bank, for the opening or operation of any Accounts, additional and/or periodic checks of the data provided by the Client/Legal Representative/Principal/Power of Attorney are required, the Bank is authorized to carry out any checks, request and obtain any information about them, as well as any other persons who make deposits in Accounts and/or have specially mandated for certain operations, from any competent authority, public register, archive, electronic database or body authorized, holder of such information. All costs related to consulting these databases, as well as any expenses, commissions and fees related to them, including postal charges, are and remain the responsibility of the Client, the Bank having an automatic debit mandate of any Client's account for their recovery.

## **3.2. Persons who can operate in the Client's Accounts**

**3.2.1.** Regardless of the number and types of Accounts, the Client who has full exercise capacity, as their holder, can appoint in relation to the Bank a maximum number of two Authorized for each Account, who have the right to have the funds from the Accounts expressly indicated by Client (performing in the case of Payment Accounts and payment operations), not having the right to request the closing of these Accounts. By exception, in the case of Term Deposit Accounts and Savings Accounts, the Power of Attorney may request the liquidation of the term deposit, respectively the closing of the Savings Account. By exception, on credit card accounts, they cannot be named as Authorized Persons.

**3.2.2** The appointment of the authorised representatives on the account, their identification data and specimen signature shall be recorded in the standard forms provided by the Bank for this purpose, as appropriate (list of authorised representatives contained in the applications form for opening a current account, the enrolment and data update forms to be completed for each authorised representative, the Specific Contract), these documents being kept by the Bank. In the event that the appointment of the Authorised Representatives is made through remote communication channels, the identification data of the Authorised Representatives on the account shall be recorded in the documents/computer applications specific to the respective access methods.

(2) The Power of Attorney given by the Client shall be considered valid until it is revoked by the Client, by one of the following means: filling in a new list of the Powers of Attorney on the current Account for which the

change will be made in the Bank's units; filling in an express request for revocation in the Bank's standard forms for other types of Accounts.

(3) The Bank may refuse the Account Representatives appointed by the Client, on the date of appointment or subsequently, if there are suspicions or reasonable grounds for suspicion of money laundering, terrorist financing, fraud, violation of International/US Sanctions and/or embargoes or in any other situation where legal or internal regulations so require. The Bank will not accept Designated Persons or Restricted Parties as Trustees on Accounts. In the event that the Bank rejects existing Authorised Representatives, it will notify the Customer in writing of the date from which the Authorised Representative is no longer accepted by the Bank.

(4) The appointment and revocation of the Powers of Attorney by the Client shall become binding on the Bank as of the working day immediately following the date of submission of the list of Powers of Attorney / request for revocation of the Powers of Attorney.

**3.2.3.** In order to be able to execute the mandate entrusted by the Client, the authorized person must provide to the Bank the information and documents requested by it and submit the Signature Specimen to the Bank.

**3.2.4.** The Customer is obliged to inform the Authorised User or the Additional Card User of these GBC and any amendments thereto.

**3.2.5.** The following persons can freely dispose, following the rules in force, on the amounts in the Current Accounts, savings or deposit opened in the Bank's record for these Clients:

a) Account holder;

b) account proxies, only during the holder's lifetime;

c) the holder's heirs, who prove with a certificate of inheritance or with a court decision this quality.

d) The users of the Extra Cards attached to the Account (only through these Cards), during the lifetime of the Account holder;

e) The legal representative of the Client, in case the Client is minor or major without exercise capacity; in this situation, in order to allow the Legal Representative to perform payment operations, he must provide the Bank with the information and documents requested by it and submit the Signature Specimen to the Bank.

### **3.3. Current Account. Savings account. Term deposit account. Credit card account.**

**3.3.1.** The Current Account is a Payment Account. The Bank may open, at the Client's request, a maximum of two Current Accounts in the same currency. Any Current Account, as offered by the Bank and requested by the Client, in accordance with the law and in accordance with the Bank's internal rules and procedures, may have attached to it Debit Cards, mobile banking service, overdraft limits or any other payment services/instruments related to the Current Account.

**3.3.2.** The savings account and the term deposit account are deposit accounts whose characteristics are detailed in the Specific Agreements.

**3.3.3.** The credit card account is an account that is opened, operated and closed under the conditions of the specific Contract and of these GBC, which has attached one or more Cards and a credit limit made available by the Bank at the request of the holder, according to Specific contract.

### **3.4. Unauthorized overdraft, granted by the Bank**

**3.4.1.** The Bank may decide to make a payment requested by the Client or to recover taxes, commissions, expenses, interest, any other amounts due to the Bank based on specific Contracts etc., which exceed the limit of the credit balance of the Current Account, even if there is no specific Contract for an account discovery facility already concluded with the Client. Thus, the mere instruction of the Bank to process Payment Orders that exceed the credit balance of the Current Account, given directly by the Client or by mandate entrusted to the Bank or through or by a third beneficiary, has the legal value of early acceptance by the Client of a non-revolving account overdraft facility ("unauthorized overdraft"), if the Bank decides to grant it at the time of payment order processing. The interest due by the Customer is calculated according to section 2.3.3, specifying that "n" is 30, and "N" is 360.

**3.4.2.** The amounts thus advanced by the Bank will be considered as due by the Client from the date of their advance and will be bearing interest calculated at an annual rate set by the Bank for such situations.

The Client undertakes to promptly supply the respective Account with all the amounts thus due, agreeing that any credit of the respective Account is considered to be made for the purpose of reimbursing with priority these amounts and that the respective amounts can no longer be reused by the Client.

**3.4.3.** For the purposes of establishing an enforceable title, the Bank and the Client agree that these GBC and the statement of account reflecting the amounts granted by the Bank under the conditions provided in 3.4.1. and 3.4.2. have the legal value of an overdraft credit agreement.

**3.4.4.** The bank has the right to recover the amounts owed without legal notice.

**3.4.5.** In case of non-payment by the Client of any amounts due on the basis of the specific Contract, the Bank will provide the Client, upon request, information about the amount of the amounts owed by the Client, not having the obligation to notify his existence and / or the value of these debts.

### **3.5. The right to compensation**

**3.5.1.** The Client hereby authorizes the Bank to compensate at any time any amount due to the Bank with the funds available in any Current Account, savings and/or term deposit, regardless of the currency in which they are available and/or regardless of the maturity of the deposit, without in this regard, another prior agreement of the Client will be necessary.

**3.5.2.** If the compensation of the amounts due will require the change of a certain currency into another, such a change will be made at the exchange rate in the account practiced by the Bank at that date, for this purpose the Bank being mandated for any foreign exchange operation that will be needed.

**3.5.3.** If the Client's Accounts are not sufficiently available to cover any amounts due to the Bank, the Bank is authorized to debit any of the Client's Accounts, even if this would generate an unauthorized account under the conditions of section 3.4. "Unauthorized overdraft granted by the Bank."

**3.5.2.** The Client will be notified by the Bank after the clearing through the account statement.

### **3.6. Termination of the current account**

**3.6.1.** The client will be able to unilaterally terminate the Current Account, anytime during the course of the specific Contract, submitting according to the rules in the "Notifications" section a written request, to any of the units of the Bank, without having to justify such a decision. The deposit accounts are denounced under the conditions of the Specific Agreement. As a rule, the current account can be closed only if at the date of the closing request there are no products and/or services offered by the Bank that require the continued maintenance of the current account, in which case the Client can resume the request to close the account only after the termination/modification, as the case may be, of the legal relationships related to the products/services in progress. The closing of the Account will be made on the date of the request; by exception, the closing of the Current Account with an attached debit card (main and/or additional card) will be made after 30 calendar days from the date on which the holder asked the Bank in writing to terminate the current Account contract, if there are recorded settlement transactions, using the form made available by the Bank for this purpose. If during this period new Card Transactions were to be settled, the 30-day deadline will be extended until all Card transactions registered on the Account.

**3.6.2** The Bank may unilaterally terminate the legal relationship of the Current Account/Savings Account /mobile banking/payment instruments attached to the Account at any time during the term of the Specific Agreement without having to justify such decision, with a written notice of two calendar months sent in accordance with the rules set out in Section 8.2 "Notices".

**3.6.3** The Bank shall be entitled to terminate the Current Account Agreement and/or the Specific Agreement relating to the services attached to the Account by operation of law, without notice and without the intervention of the courts, in any of the following cases:

**a)** the Client does not comply with the legal provisions in force, the Bank's working rules or the Account's operating conditions;

**b)** there is reasonable suspicion regarding the Client's direct or indirect involvement in operations that contravene legal provisions on the prevention and combating of money laundering, terrorist financing, and international/US sanctions. The suspicion also concerns situations in which the Customer becomes a Designated Person or Restricted Party, or is subject to International Sanctions, including those imposed by the US, the

European Union, or other states, international organizations, or their agencies, regardless of whether they are directly or indirectly targeted;

**c)** there are suspicions or reasonable grounds for suspicion of fraud/money laundering/terrorist financing/violation of International/US Sanctions/illegal activities as provided for by applicable criminal law and/or other applicable regulations or in the event that requests for return of funds were received from the ordering/correspondent banks on the grounds of suspected fraud/money laundering/terrorist financing/violation of International/US Sanctions or information on suspected fraud/money laundering/terrorist financing/violation of International/US Sanctions against the Client from the Romanian or foreign authorities, from banks in Romania or abroad;

**d)** the Client has provided the Bank with insufficient/unreliable information and/or documents or refuses to provide the Bank with the information and/or documents and/or agreements necessary for the Bank to fulfil its contractual and/or legal obligations (including for the purpose of applying FATCA and/or CRS requirements);

**e)** the Account balance no longer covers the costs related to the execution of the specific Current Account Contract;

**f)** in the case of "dormant" Accounts covered in section 3.7;

**3.6.4** In the cases provided in art. 3.6.3 letters a), b), c), d), f) above, the Bank will notify the Client of the measure taken, within no more than 5 working days from the taking of this decision, according to the rules of section 8.2. "Notifications". In the cases provided in art. 3.6.3 letters e) the closure of the Account is made without notification.

**3.6.5.** In all the cases in which the initiative of closing the account belongs to the Bank, as of the closing date of the account, the Bank will cease crediting the account with interest, and the amount which would represent the credit balance of the Account on that date would be made available to the Client into non – interest- bearing accounts. The Client owes the standard fees/commissions related to the payment operation of the sums of money, as provided for in Fees and Commissions into force upon carrying out the operation. The Bank will not be liable under any circumstance for potential direct or indirect damages that the Client might incur as a result of the closing of his/her accounts, according to the afore mentioned.

**3.6.6** The Term Deposit/Savings Account Agreement shall automatically terminate in the event of termination for any reason of the Current Account Agreement opened in the currency of the savings product with the Bank. In this case, the termination of the term deposit/savings account shall take place on the same date as the date of termination of the Current Account contract and the Customer agrees that the Bank shall proceed to transfer the amount of the deposit/savings account to the respective Current Account after liquidation of the deposit/savings account with this date, even if it has not reached maturity and with interest rate subsidy until the date of termination of the deposit/savings account contract.

**3.6.7 (1)** The Specific Contracts shall terminate in the cases and under the conditions mentioned therein, which shall be supplemented with the cases of termination of the account relationship provided for in art. 3.6.3 of this document.

**(2)** The provisions of the GBC shall apply until the date on which the Client no longer has any Specific Agreement in force with the Bank, from which date the business relationship with the Bank shall be deemed to be terminated. However, any claims, requests, disputes, litigations, demands submitted/introduced by the Client after the date on which the business relationship with the Bank has ceased or which have been previously initiated and are ongoing at that date, will be analyzed in relation to the provisions of the Specific Contract and/or the GBC in force on the date on which the act/obligation claimed/requested/contested by the Client was concluded/occurred/performed.

### **3.7 Special provisions applicable to “dormant” accounts**

**3.7.1** If during a period of time, determined by the Bank and made known to the Customer by posting at the Bank's units and on the Bank's website, no request by the Customer to change the Account has been registered and approved for the Current Account or Savings Account, or if no debit or credit transaction has been made to the Account by the Customer, third parties or the Bank, the Account shall become "dormant".

The time period set by the Bank for a Current Account to become "dormant" is general and applies to all Current Accounts.

In this case, the Bank will continue to charge fees and commissions to the respective accounts as long as there is a credit balance. The Bank will also continue to calculate the credit/debit interest according to the characteristics of each Account as long as there is a credit/debit balance.

**3.7.2** By way of exception to the provisions of art. 3.6.4 above, the Bank may at any time decide to close the Account declared "dormant" with zero balance or debtor, without the Client's prior or subsequent notification.

**3.7.3** Following the approval of a request to modify an account or after processing a debit or credit transaction on the "dormant" Account, it will be reactivated automatically by the Bank; After approving the request to modify the Account/carrying out the transaction, the Account will remain in an "active" state and may become "dormant" under the conditions mentioned in this section.

**3.7.4** The Bank shall not notify the Customer of the Account going into "dormant" status.

Debit or credit operations carried out by the Bank, representing exclusively the payment of interest by the Bank and the payment of commissions/fees related to the Account, are not considered as Account movements.

### **3.8 Account blocking.**

**3.8.1.** The Client's Current Accounts may be blocked (i) totally, in which case no Payment Transactions (deposit/withdrawal of funds, transfer of funds, collection) will be executed or (ii) partially, in which case only the Payment Transactions of crediting the Current Account (collection) will be executed.

**3.8.2. (1)** The Bank is entitled to order the total or partial blocking of the Accounts in any of the following situations:

**a)** compliance with the Bank's customer acceptance and KYC policies and the legal provisions on preventing and combating money laundering and terrorist financing, legal provisions regarding International Sanctions, as well as the legal provisions on preventing and combating fraud;

**b)** suspicion of fraud, suspicious, unauthorized or illegal transactions on the Current Account;

**c)** for any objectively justified reasons related to the security of the Current Account and compliance with the legal provisions in force;

**d)** in any other cases provided for by these GTC and the legal provisions in force;

(2) The Client may request the Bank to block the Current Accounts in case of suspicion of fraud, suspicious, unauthorized or fraudulent transactions.

**3.8.3 (1)** During the partial blocking of the Current Account: **(i)** credit or debit interest shall be calculated and recorded; **(ii)** the Account administration fee provided for in the Specific Agreement shall be charged; **(iii)** any Payment Transactions completed by crediting the Current Account shall be recorded; **(iv)** the Bank shall not execute payment orders that have the effect of debiting the Current Account.

**(2)** During the total blocking of the Current Account: **(i)** no Payment Transactions (deposit/withdrawal of funds, transfer of funds, collection) shall be executed; **(ii)** no Account administration fee provided for in the Specific Agreement shall be charged; and **(iii)** no interest shall be calculated and recorded as a credit or, as the case may be, as a debit.

**3.8.4** In the event that the Current Account is blocked as provided above, the Bank may also block any payment instrument/service giving access to such Account.

**3.8.5 (1)** In the situations referred to in paragraph 3.8.2 para. (1) above, the Bank shall be entitled to block the Client's Deposit and Savings Accounts.

**(2)** During the blocking of the Deposit and Savings Accounts: **(i)** the Client shall not be able to make partial or total withdrawals of funds; **(ii)** the other contractual provisions shall apply under the conditions provided for in the specific Contracts.

### **3.9 Provisions regarding interest, taxes and commissions related to the current account**

**3.9.1.** The credit interest is calculated according to section 2.3.3., specifying that "n" is the actual number of days for which the interest is calculated and "N" is 365/366. The credit interest is calculated daily for the balance existing at the end of the banking day. Interest is calculated for the calendar month and year and will be credited monthly, capitalizing on the account. Interest credit is only made after deducting the interest income tax according to the legal provisions in force.

**3.9.2** The administration fee of the current account is due monthly on the last working day of the month, for the month during which it is due to pay it, in the absence of a contrary provision in the request for opening an account.

The administration fee of the Current Account is charged pro-rata both in the month of opening and in the month of closing of the Current Account, in proportion to the period when the Account was opened.

**3.9.3** The Bank is authorized by the Client to debit the Current Account, at the maturity of any tax/commission related to it, with the amount necessary to pay. Partial payments are also accepted. If there is not enough available in the current account for the total payment obligation to be cancelled, the provisions of art. 3.4 regarding the discovery of unauthorized account granted by the Bank and art. 3.5 regarding the right of compensation in these GBC.

### **3.10 Prescription term**

In all cases where an Account is closed, the term within which the Client will be able to request the refund of the amounts that represented the credit balance of the respective Account at the date of its closing, is the legal limitation period that begins to run from the date on which the notification of closure of the Account it is considered received by the Client according to section 8.2. "Notifications". If the law does not provide for a specific notification method, it will be done according to the provisions of section 8.2. "Notifications". During this period, the amounts recorded in the balances of the closed accounts will be kept by the Bank at the disposal of the Client, in interest-bearing accounts.

## **4. PROVISIONS REGARDING PAYMENT OPERATIONS**

In case of conflict between the provisions of this chapter and those of the Specific Contracts regarding the payment operations and the Payment Accounts, the rule stipulated in point 1.2.1 applies. By way of exception, the provisions of this chapter modify and/or duly complete, where appropriate, the Specific Agreements regarding the payment operations and the Payment Accounts concluded before 15.12.2009.

Clients who opened an Account accessible online have the possibility to initiate payments, to obtain information about this account or to obtain any information regarding the availability of funds through third party service providers, being able to use the security elements provided by the Bank for this purpose. Aspects related to the use of the services offered by third-party payment service providers are regulated in the specific contract for Smart Mobile service.

### **4.1 Account unique identification code**

**4.1.1.** In order for the Bank to execute a Payment Order in relation to a Payment Account, the Customer shall provide the Bank with:

- a)** the IBAN code of the Payment Beneficiary's Account (or the BBAN - basic bank account number - for countries that have not joined the IBAN); for payments ordered to beneficiaries whose service providers are established outside the European Union next to the IBAN/BBAN code of the Payment Beneficiary's Account, the Client will provide the Bank and the name and surname of the payment beneficiary;
- b)** for foreign currency payment transactions, except for payments in Euros made within the EU/EEA when the beneficiary account is identified through IBAN, additionally to the information from letter a) above, the name and address of the payment service provider of the payment beneficiary or the BIC/SWIFT (Business Identifier Code) code of this provider must be provided; if the Client provides to the Bank both the name of the payment service provider of the payment beneficiary and the BIC/SWIFT (Business Identifier Code) code, when applicable, of this provider, the Bank will use only the BIC/SWIFT (Business Identifier Code) in order to send the payment to the provider. The Client understands and accepts that in order to execute a payment order in connection with a Payment Account, ordered by it, the Bank will communicate to the beneficiary's bank, the IBAN code of the paying account, the Client's name and surname and his/her address/residence address in track recorded in the Bank's database and validated on a documentary basis, by including them in the information accompanying the transfers of funds.

**4.1.2.** The Bank has in no case the obligation to verify the name of the Account holder indicated as beneficiary by the Client in the payment order and also his Account number, making the payment in the account indicated in the payment instruction.

**4.1.3.** In order to process the payment instructions, upon taking over the IBAN codes transmitted by Clients in the Bank's information systems or taking the IBAN codes represented on paper in the internal systems, the Bank has the obligation to validate the IBAN codes of all the Accounts mentioned in the payment instructions they process, using the validation method imposed by the legal regulation in force. In addition, the Bank will validate the BIC codes of the beneficiaries' service providers when the BIC codes are required, mentioned in the payment instructions sent by the Bank's Customers, using the validation method required by the legal regulation in force, as well as the concordance between the IBAN code that identifies the payment beneficiary and the BIC code of the payment service provider of the beneficiary indicated on the payment order, when the BIC code is required, verifying the location of both codes (IBAN and BIC) in the same country and/or at the same payment service provider.

**4.1.4.** In order to credit the Paying Account of a beneficiary Client, the Bank will verify:

**a)** the existence of the information regarding the payer, within the payment details as they were communicated by the provider or the payment services (the name of the payer and the unique identification code of the payment account of the payer and, in addition, the following additional information: the payer's address or the document number official payer personnel or payer identification number or date and place of payer birth, all such additional information only if either the payer's payment service provider or the intermediary payment service provider, if applicable, is established outside space of the European Union)

**b)** the existence and accuracy of the information regarding the Beneficiary Client (the unique identification code of the beneficiary's payment account and, in addition, the beneficiary's name for either the payment service provider of the payer or the intermediary payment service provider, if applicable, is established outside the EU/EEA area).

**4.1.5 (1)** In the case of Payment Orders, in foreign currency, transmitted to a Payee Customer's Payment Account, received by the Bank from another payment service provider located outside the European Union/European Economic Area, the Bank may perform additional checks in accordance with its legal provisions/internal procedures (such as, but not limited to: correspondence between the name of the Payee Account holder and the Account number indicated in the Payment Order, existence of the payer's complete address - country, city, street, number), in order to process the Payment Order correctly.

**(2)** In order to carry out the checks referred to in the previous paragraph, the Bank may request additional information from the ordering/correspondent bank. If the Bank does not receive the requested information or receives incomplete information or if it contains discrepancies with the information held by the Bank on the Payee Customer, the Bank shall not process the Payment Order.

## **4.2 Authorise payment orders**

**4.2.1. (1)** The Bank shall provide the following channels to Customers for initiating Payment Orders:

**a)** mobile banking service, according to the specific Contract;

**b)** terminals (ATMs/MFMs) for Payment Transactions initiated/authorized through the Card;

**c)** other channels/applications for making payments on the basis of Specific Contracts concluded with the Client.

**(2)** In any of the following situations: (i) the non-functioning of mobile banking service for periods longer than three hours; (ii) in the situation where the mobile banking service is blocked at the Bank's initiative, without also blocking the accounts; (iii) in the situation where the Customers request the performance of currency exchange operations on the account at a negotiated exchange rate; (iv) in the situation where the Customer's accounts are seized; (v) in other situations where the Customer invokes the impossibility of using the channels mentioned in lit. a) - c) deemed justified by the Bank, the Clients may initiate, by way of exception, Payment Orders (including foreign exchange) on paper in the Account, in any of the Bank's units.

**(3)** The Bank accepts only editable payment order forms with bar code for transactions in lei and editable payment order for payment transactions in foreign currency and external payments in lei, being necessary to download the forms accepted by the Bank from the website [www.raiffeisen.ro](http://www.raiffeisen.ro), to fill them in electronically, to sign them by hand and to present them in original, on paper, in the banking units.

(4) The Bank has the right, but not the obligation, to refuse the execution of payment orders/currency exchanges to the Account, initiated on paper, in situations other than those mentioned in paragraph. (2). (i) - (v) and may not be held liable for such refusal; the Bank may also not be held liable if it accepts the execution of paper-based Payment Orders/currency exchanges in the Account in situations other than those mentioned in para. (2) item. (i) to (v) of this Article.

(5) The Bank may also provide the Client with other channels for the transmission of payment orders, to the extent it has expressly agreed with the Client under a Specific Agreement.

**4.2.2** A payment operation is considered authorized only if the Paying Client has expressed its personal consent or through legal representative, as the case may be, through the authorized person, for the execution of the payment operation in one of the modalities listed below and which will be supplemented, if necessary, with the regulations of the Specific Agreement:

**a)** in writing, on paper, by applying the signature of the Client/Proxy on the payment form/on the Specific Agreement, in accordance with the signature specimen deposited with the Bank.

**b)** by affixing the electronic Signature on the payment order in electronic format under the terms and conditions agreed upon under the specific Agreement related to such a payment instrument;

**c)** by telephone, under the conditions of the Specific Agreement, after completing the special procedure for identifying the Client.

**d)** by using the security elements (such as PIN, passwords, authentication code, etc.) according to the Specific Agreement.

**e)** by communicating the identification data of the Cards requested by the beneficiaries of the payment services and possibly, of some security elements, in the terms and conditions agreed with them.

**4.2.3.** The Client accepts that the Bank may perform Payment Operations from its Accounts without its express consent or agreement, to pay the amounts established by final or arbitrary judgments and/or other enforceable titles provided by law, irrespective of the state budget, budgets. local or any third party, to correct the errors found when checking the transactions in the Account, as well as to retain the commissions/other amounts owed/due to the Bank for the operations performed/in connection with them, the interest and the outstanding and/or outstanding credit rates or in any other cases provided by law, these payment operations being considered authorized by the Client, within the meaning of the previous article.

**4.2.4** In the event of a garnishment on the Client's accounts, if the law does not prohibit the Bank from doing so, the parties agree that the Bank may inform the Client by email and/or SMS (to the email address and/or mobile phone number declared to the Bank) or by another means chosen by the Bank, regarding the establishment of the garnishment on the Client's accounts.

### **4.3. Execute payment orders**

**4.3.1.** The Bank will execute the payment orders received from the Client only if the following conditions are met:

**a)** the payment order is submitted by the Paying Customer, if applicable by the Payee Customer, on the standard forms issued by the Bank - payment orders with barcode or required by law, or through the electronic channels offered by the Bank, is completed with all mandatory elements, is legible and authorised or signed by the Customer/Authorised Representative in full accordance with the Specimen Signatures held by the Bank (in the case of payment orders with barcode issued on paper);

**b)** depending on the type of payment instrument used to transmit the payment order, the Client initiating the payment operation provides all the information requested by the Bank according to the specific Contract and/or through the payment forms accepted by the Bank.

**c)** In the case of bar code payment orders, the information transposed from the bar code of the payment order corresponds to the information entered on the payment form; in case of inconsistencies, the information on the form will prevail;

**d)** The funds available in the Payment Account are sufficient to allow both the respective payment and the payment of commissions due to the Bank for the services provided, except for the offline electronic payments, in case you cannot query the balance of the Payment Account at the time of payment by the Customer ;

- e) The ordered payment orders do not contravene the applicable legal regulations (for example: in the ordered payment operations are not involved goods, persons and territories in relation to which are disposed, according to the law, international sanctions for blocking funds, currency regulation etc.)
- f) The paying Customer or the beneficiary of the payment is not registered in a list of persons subject to a ban on the use of bank accounts/making of payments/international bonds/US freezing of funds/other related legal measures taken for the purpose of preventing and combating money laundering, terrorist financing and/or the Bank has no suspicion or there are no reasonable grounds for suspicion of fraud/money laundering/terrorist financing/non-compliance with International/US Sanctions in relation to the Payment Transaction, so as to consider that the refusal to execute the Payment Transaction is necessary for the prevention of possible fraud, breaches of law, etc. ;
- g) the payment identification codes mentioned in art. 4.1 are validated by the Bank, according to the provisions of art. 4.1.3
- h) the cas available in the Payment Account necessary for the execution of the payment order is not affected by a measure of unavailability of the account/blocking of the funds taken by the Bank based on some legal provisions or the conventions existing between the parties, under an enforceable title or disposed of by an organ having such competences, representing, but not limited to: confiscation, insurance confiscation, forced execution, seizure, distraint, the establishment of mandatory international sanctions in national law, the application of a sanction by the Bank.
- i) there are no reasonable reasons for the Bank to doubt the authenticity of the Payment Order regarding the source, content, signature, consent, etc.
- j) The Customer complies with the requirements of point 4.3.8
- k) The Bank has not received transaction restrictions on the Client's accounts from Correspondent Banks and/or requests for return of funds from Ordering / Correspondent Banks on the grounds of suspected fraud, money laundering, terrorist financing or non-compliance with International / US Sanctions;
- l) in the case of transactions related to Virtual Coins, the Bank shall receive from the Client the requested supporting documents regarding the source of funds invested in Virtual Coins;
- m) transactions are not carried out with providers of exchange services between Virtual Currencies and fiat currencies and/or Digital Wallet Providers that are unauthorised/unregistered or from countries designated by the European Union as high-risk third countries and/or non-cooperative jurisdictions for tax purposes;
- n) The Customer does not conduct transactions with payment service providers from countries designated by the European Union as high-risk third countries and/or non-cooperative jurisdictions for tax purposes;
- o) the payment transaction initiated by the Customer has not been restricted/limited by the Bank in application of the measures set out in points 3.1.4 (ii) and (iii).

**4.3.2.** The Bank is entitled not to carry out any transaction which presents a risk of legalizing the revenues from the financing of terrorism or which raises suspicions regarding the incidence of national and international sanctions on the financing of terrorism, or if it considers that it does not comply with the legal regulations in this area. The Bank may refuse the instructions of the Client to transfer funds to financial institutions/individuals/legal entities in countries suspected of supporting terrorist actions or subject to International Sanctions/Embargoes, classified by national/international authorities or international institutions/organizations or to financial institutions outside such territories, whose parent company is registered in a country on such a list. The list of these countries can be consulted on the Bank's website, [www.raiffeisen.ro](http://www.raiffeisen.ro).

**4.3.3** If several payment instructions are ordered by the Client, whose total amount exceeds the credit balance of the Payment Account or the maximum amount of any type of overdraft granted to the Customer, the Bank will execute the payment operations within the limit of the available balance and in the order processing of instructions for internal processing systems.

**4.3.4.** The client assumes the obligation to keep in the Payment Account the availability necessary to execute the payment order until the expiry of the execution term indicated by the Bank for the ordered payment operation.

**4.3.5.** The trading limits imposed by the Bank for the use of a certain payment instrument, if any, are those established in the Specific Agreement.

**4.3.6.** Cash transactions (deposits or withdrawals) may only be carried out at ATM/MFM terminals by Customers holding a Card and shall be recorded and executed by the Bank in accordance with the legal provisions applicable to payment services and the contractual provisions agreed by the parties.

**4.3.7.** Information on the limits of cash deposits and withdrawals, in lei or in available currencies, which can be made at the Bank's ATMs/MFMs, is available on the Bank's website [www.raiffeisen.ro](http://www.raiffeisen.ro), in the section "In your support". The Customer may request an increase of the cash withdrawal limit in lei or in foreign currency according to the information that the Bank provides in the same section of the website.

**4.3.8.** In executing payment instructions, the Bank shall act in good faith and exercise reasonable diligence, determined in accordance with the standards, banking practices, national and international customs, uniform rules and any applicable national and international regulations, which shall duly supplement these GBC and shall together govern the legal relationships to which they apply;

For the payment transactions initiated, regardless of the method of their transmission, the Customer is obliged to submit to the Bank, at its request, supporting documents in accordance with the requirements of the legislation in force.

The Bank shall carry out the checks required by the applicable legislation, as well as additional checks in the event that it has reasonable grounds for suspicion or reasonable suspicion regarding fraud, money laundering, terrorist financing, violations of International/U.S. Sanctions, or when such suspicions have been communicated to the Bank by other credit institutions, financial institutions, payment service providers, or authorities. The amounts related to such transactions shall be blocked until the completion of the checks, and the execution deadlines may be extended accordingly. **4.3.9.** The Bank shall be entitled to use communications, settlement or payment systems or the services of a third party to execute the Payment Operations ordered in the Payment Accounts.

**4.3.10.** The Bank will not be liable to the Client for any delay or deficiency of a third party (including, without limitation, intermediary banks, agents, notaries public, court executors, etc.) in fulfilling its duties in relation to the Bank, even if the delay or deficiency does not occur in abnormal and unforeseen circumstances, outside the control of the person invoking them and whose consequences could not have been avoided in spite of all due diligence in this regard or if the third party is obliged to comply with other legislative provisions.

**4.3.11.** In the case of the amounts in the currency transferred to the Paying Account of a Beneficiary Client if the Beneficiary Account mentioned in the Payment Order is opened in another currency The Bank will execute the payment operation by crediting the Beneficiary Account with the currency equivalent of this Account of the transferred amount, calculated at the Course exchange rate of the Cross-currency Bank from the moment of crediting the Account.

**4.3.12.** In the case of the amounts in the currency transferred from the Payment Account of a Paying Client, if the Paying Account mentioned in the payment order is opened in another currency, execute the payment operation by debiting the Paying Account with the currency equivalent of this Account of the transferred amount, calculated at the Bank's Exchange rate, as indicated by the Bank at the time of receiving the payment instruction and accepted by the Paying Client.

**4.3.13.** The Bank does not perform transfer operations of the amounts in lei from the Accounts in the currency of the Paying Client, nor any operations to collect the amounts in lei transferred to Accounts in the currency of the beneficiary Client.

**4.3.14** If the payment order through which amounts are transferred to the Paying Account of a beneficiary Client is revoked by the payer, with the acceptance of the beneficiary Client, after the Bank has credited the beneficiary Client's account, in the case in which the transferred amount was expressed in a currency other than the one of the beneficiary Account and the Bank performed the currency conversion according to the provisions of art. 4.3.12, the Bank will refund the amount that is the object of the payment order revoked, in the currency indicated in the payment order, the Paying Client bearing the eventual exchange rate differences resulting from the conversion made between the amount credited to the beneficiary Client's Account and the amount transferred to the payer who revoked the payment order; in this situation, the conversion will be carried out at the exchange rate of the cross-currency bank from the moment of the debit of the beneficiary client's account.

#### **4.4. Terms of execution**

**4.4.1.** The Bank will execute the Payment Operations in compliance with the following terms:

**Raiffeisen Bank S.A.** • Bank's headquarters in FCC Office Building, Calea Floreasca No. 246 D, District 1, Bucharest • Postal code 014476 • Romania • Phone: +40 21 306 1000 • Fax: +40 21 230 0700 • E-mail: [centrala@raiffeisen.ro](mailto:centrala@raiffeisen.ro) • [www.raiffeisen.ro](http://www.raiffeisen.ro) • Unique registration code 361820 • Trade Registry No. J1991000044406 • EUID ROONRC.J1991000044406 • Banking Registry No. RB-PJR-40-009/1999 • FSA Capital Markets Public Registry no. PJR01INCR/400009/30.01.2014; PJR24DIST/400009/01.03.2016 • FSA Private Pension Public Registry code AMJ-RO-374277 • Affiliated Agent registered to FSA under Code RAJ 500196 • Fiscal registration code RO361820 • Share capital Lei 1,200 Mio subscribed and fully paid-up • Company administrated in dualist system • Call Center: \*2000, standard call rates apply to all mobile networks in Romania.

- a) for the national operations in payment in lei: at the latest until the end of the next working day after the day of receiving the Payment Order;
- b) for payment operations denominated in Euro or other official currency of a Member State of the European Union or of the European Economic Area ("EU/EEA") outside the euro area, when the payment service provider of the beneficiary is located in a EU/EEA member state: at the latest by the end of the next working day after the day of receipt of the Payment Order;
- c) for payment operations in any currency other than those of EU/EEA Member States, where the payee's payment service provider is located in an EU/EEA Member State: at the latest by the end of the third business day after the date of receipt of the Payment Order;
- d) for payment operations in any currency, when the payment service provider of the payment beneficiary is not in an EU/EEA Member State: at the latest by the end of the third working day after the day of receipt of the payment order;

The payment operations provided for in letters a), b) and c) above are considered executed on the date of the credit of the payment service provider's account of the payment beneficiary with the amount of the Payment Operation. The payment operations provided for in letter d) are considered executed by the Bank at the moment when the Bank transfers the money to the payment service provider's account of the Payee Beneficiary through the corresponding banks and/or through the external settlement systems.

**4.4.2** In the case of Payment Transactions carried out through Correspondent Intermediary Banks and/or through External Settlement Systems in other countries, for the calculation of the deadlines referred to in the previous point, the days established as non-working days and the national legal holidays of the respective countries shall not be taken into account and, as a result, the execution deadlines shall be extended accordingly to the number of such days.

**4.4.3.** The Bank has no obligation to credit a Payment Account before receiving the appropriate final payment, unless it has otherwise agreed with the Client in the Specific Agreement.

In the case of currency payment transactions, the Bank will credit the Beneficiary Client's Account as appropriate:

- (i) for interbank operations, depending on the Time limit, as the case may be, on the day on which the Bank's account was credited or on the next business day, the operation with the Effective Date on which the Bank's account was credited shall be recorded in the Account;
- (ii) for in-bank operations, on the day of the payment instruction execution.

**4.4.4.** Cash deposit and withdrawal transactions at ATMs/MFMs are processed by the Bank online and are recorded in the Payment Account immediately after the transaction is completed.

**4.4.5.** If the payment instructions that have as effect the credit/debit of a Payment Account are sent to the Bank on non-working days, it will be shown in the Account balance in the first working day following.

**4.4.6** At the Client's request, the Bank executes the Payment Operations before the fulfilment of the maximum execution term provided in art. 4.4.1, in which case the Customer owes to the Bank the additional tax for the emergency regime.

## **4.5 The refusal to execute payment orders**

**4.5.1 (1)** If the Bank refuses to execute a Payment Transaction (e.g. deposit/withdrawal of cash, transfer/collection of a sum of money, etc.), the refusal and the reasons for the refusal shall be communicated to the Client within the execution deadlines corresponding to the payment transaction ordered, specified in section 4.4, in the manner specific to each product/service,

- a) at the Bank's units, at the Client's request for direct debit or scheduled payment order services;
- b) via payment instruments (such as mobile banking);
- c) by means of specific devices that make it possible to execute payment transactions ordered through payment instruments (such as ATM, MFM, EPOS, etc.);
- d) through the operator of the phone banking service offered by the Bank.

**(2)** As an exception to the preceding paragraph, the Bank shall not inform the Customer of the refusal and/or the reasons for the refusal to execute a Payment Transaction if this is prohibited by national or international legal provisions (including but not limited to legal provisions relating to suspected fraud, money

laundering/terrorist financing/violation of International/(US) Sanctions) or has been requested by competent authorities or for security and fraud prevention reasons.

#### **4.6 Revoke payment orders.**

**4.6.1.** Once expressed by the Client, in the corresponding ways mentioned above, the consent is irrevocable, after the Payment Order has been received by the Bank. By exception, in the case of direct debit type services, the consent given for the execution of several Payment Operations may be withdrawn at the express request of the Customer, formulated in writing and deposited at any territorial unit of the Bank, at the end of the business day preceding the agreed day at the latest, for debiting Payment Accounts, following which any other future payment transaction will be deemed unauthorized.

**4.6.2.** The Bank will be able to accept, at the Client's request, the necessary steps to revoke the Payment Orders instructed by the Customer after the payment authorization (the Customer expressing the consent regarding the payment operation), only if the following conditions are cumulatively met:

- a) The Client completes the specific form provided by the Bank for the purpose of revocation;
- b) The Client pays the commission related to the requested operation;
- c) The payment order has not yet been executed;
- d) The currency of the payment transaction is expressed in lei and the payee's bank is located outside Romania or the currency of the payment transaction is in foreign currency and the payee's bank is located in Romania or outside Romania.

**4.6.3.** The Bank cannot guarantee the successful revocation of a Payment Order if:

- a) the payment instruction has already been sent to the beneficiary's bank in the case of interbank payment operations.
- b) the amount of the transaction has already been credited to the Payee's Account in the case of interbank payment transactions; In this case, the revocation will be possible only with the agreement of the beneficiary of the payment.
- c) The currency of the payment transaction is expressed in lei and the beneficiary's bank is located in Romania.

**4.6.4.** Any occasional cost or injury suffered by the Bank, arising from the revocation or modification of a Payment Order, will be borne by the Client and automatically debited by the Bank from any of its Account, without completing any other formalities.

#### **4.7. Provisions regarding the price, interest rate and the exchange rate. Commissioning options applicable to payments**

**4.7.1.** When the payment service provider of the payment beneficiary is located in a member state of the European Union/European Economic Area (EU/EEA), the payment operations in lei or in any currency are instructed with the SHA commissioning option.

**4.7.2** If the Paying Client expressly indicates, on his own responsibility, the OUR commissioning option, the Bank may accept to execute a payment of the nature of those of art. 4.7.1 above, instructed in a currency that does not belong to an EU/EEA Member State, the Client agreeing to bear all the costs related to the transfer of the entire amount subject to the payment instruction.

**4.7.3** The paying customer cannot use the BEN commissioning option for the Payment Operations provided in art. 4.7.1 above, as a result, if the Bank receives Payment Orders instructed with the BEN option in favor of a beneficiary whose payment service provider is in an EU/EEA Member State, it will process the payment with the Option of SHA commissioner.

**4.7.4** When the payment service provider of the Payee Beneficiary is in a state outside the EU/EEA, the Client may choose to apply any commissioning option: SHA, OUR, BEN.

**4.7.5** For the services provided, the Client owes the Bank a price in the form of taxes, commissions, expenses and/or any other costs mentioned in the specific Contract regarding the payment service.

**4.7.6** If the Client is the Beneficiary of the payment, he agrees that the Bank may collect from the transferred amount the costs due by the Client to the Bank for the execution of this Payment Operation.

**4.7.7** For the payment operations carried out by the Card which also involves the exchange of a currency, the Reference Exchange Rate will be applied as indicated in the specific Contract regarding the payment service.

**4.7.8.** In the case of payment transactions involving a currency exchange and currency exchanges made by the Client through the Current Account, the exchange rate applied by the Bank at that time or, where applicable, the one negotiated with the Client shall be used; the exchange rate applied by the Bank shall be communicated to the Client by displaying it on the Bank's website [www.raiffeisen.ro](http://www.raiffeisen.ro), at the Bank's territorial unit headquarters, by displaying it in the specific mobile banking application or through the Bank's operator, in the case of phone banking.

**4.7.9.** For the collection of commissions involving a foreign exchange, the exchange rate of the Bank valid at the date of commissioning will be applied, unless otherwise agreed in the Specific Agreement.

**4.7.10.** The parties agree that the changes regarding the Interest Rate, the Reference Exchange Rate and the Currency Exchange Rate of the Bank provided in the specific Contract regarding the payment services, as the case may be, will apply immediately and without any prior notification.

**4.7.11.** The Client agrees that the Bank shall apply immediately and without any prior notification the changes in the Interest Rate or the Currency Exchange Rate applied by the Bank, when these are more advantageous to the Client.

**4.7.12.** The parties agree that the information regarding the exchange rate/interest rate applied by the Bank in the case of payment services, as well as the changes in the reference exchange rates or the reference interest rates applied by the Bank for the payment services, shall be communicated to the Client in the contents statement of account.

#### **4.8. Provisions regarding the communication by the Bank of the mandatory information regarding the execution of a payment operation**

**4.8.1.** The information regarding the debit/credit of the Payment Account will be made available at the latest on the working day following the debit/credit.

**4.8.2.** The communication of the mandatory information regarding the execution of a Payment Operation will be made according to the specificity of each product/service, in one of the following ways:

**a)** in the case of mobile banking service: by posting in the specific application of some text messages or by generating an electronic confirmation;

**b)** in the case of the telephone banking service: by voice message communicated by the operators of the service under the conditions of the specific Contract, or by voice message communicated by the automatic operator in the case of the automatic functionality of this service, or by a specific document sent personally, at the headquarters of the Bank's agencies;

**c)** in the case of Debit/Credit Cards: by displaying text messages and/or generating paper receipts by electronic devices through which the card is used (eg ATM, EPOS, Imprinter) and, on request, by voice message communicated by to phone banking service operators;

**d)** in the case of Payment Operations initiated on paper support, as well as in the case of scheduled payment order services, direct debit: on paper support, in the Bank's territorial units;

**e)** in the case of the mobile banking type service through the intermediary extract obtained by the Client according to the specific Contract.

**4.8.3.** The generation of duplicate Payment Orders related to the transactions carried out through the phone banking service shall be made only at the Client's express request addressed to any territorial unit of the Bank.

**4.8.4.** For the record of the payment operations, registered in the Client's Payments Accounts, the Bank will issue and communicate to it monthly, the statement of account (in the case of the credit card, in the Activity Report).

The statement of account will also highlight the corrections made by the Bank for any error found in connection with the operations performed in the Account.

**4.8.5.** The Bank shall ensure the free communication of the monthly account statement in one of the following ways:

**a)** at any territorial unit of the Bank, on paper at the Customer's request;

**b)** through the mobile banking service, during the period when this service is active in electronic format; **4.8.6.** The Bank ensures the communication of the monthly account statement, on paper, by post, only if the Client opts for this method of communication, in which case the Client owes the fee provided in the specific Lists; in order to waive this way of communication, the Client must make a written request expressly for this purpose

and indicate another free way of information, among which can be made available by the Bank. The activity report issued by the Bank for the credit card will be communicated according to the provisions of the Specific Agreement. The Bank offers the Client the possibility to choose, for the communication by post of the monthly account statements for the Current Accounts, a separate postal address for each Current Account separately, different from the Home Address or the Correspondence Address chosen by the Client for the communication of any other Notifications, according to article 8.2 of this document.

**4.8.7.** In order to issue any documents containing information of the history account statements, or, as the case may be, the provision of any other services relating to the account statements, the Bank may charge a commission, the value of which is that mentioned in the Specific Agreement.

**4.8.8.** The client expresses its agreement that, if it benefits from the mobile banking service, it will be notified of the monthly account statement, free of charge, only in electronic format, exclusively through the specific application.

**4.8.9.** The client accepts that the statements of account transmitted in any manner agreed with the Bank in accordance with these CBG and/or in the Specific Contracts, as well as any other extracts from the Bank's records, prove conclusive and correct in some legal procedures, or for other purposes, both regarding their content, as well as of the Client's obligations, unless they contain a clear error, proven with a written document having a definite date.

**4.8.10.** The power of attorney on the account is not entitled to request an account statement, but only information regarding the account balance and the operations performed by it on the Account of the holder.

**4.8.11** The Bank makes available to the Client, once a year, free of charge, a statement of all the commissions related to the Account, incurred during a previous period of 12 months. The situation of the commissions made available to the Client can be accessed through the mobile banking service or can be requested, on paper, in any territorial unit of the Bank.

#### **4.9. Provisions regarding security requirements**

**4.9.1.** The payment instructions given to the Bank will be executed at the Client's account and risk, which will bear the consequences resulting from misunderstandings or errors in all cases where the Bank is not held liable, according to the law.

**4.9.2 (1)** The Bank acts in accordance with the provisions of national and international laws and regulations on sanctioning money laundering and preventing and combating the financing of terrorist acts, the implementation of International/US Sanctions, imposed on certain states, entities and persons, and in accordance with regulations relating to:

**(i)** restrictions on dual-use item transactions (export, transfer within the European Union, brokering services, technical assistance and transit, having as their object: items, including software products and technology, which can have both civilian and military use, and which include items which can be used for the design, development, production or use of nuclear, chemical or biological weapons or delivery vehicles for such weapons, including all items which can be used both for non-explosive purposes and to contribute in any way to the manufacture of nuclear weapons or other nuclear explosive devices).

**(ii)** restrictions on operations with military goods (export, import and transfer, on a permanent or temporary basis, from or into the territory of Romania, intermediation, transit through Romania, transshipments carried out on the territory of Romania concerning any of the goods on the List containing the categories of military goods subject to the regime of control of exports, imports and other operations, set out in the Annex to Government Emergency Ordinance no. 158/1999 *on the regime of control of exports, imports and other operations with military goods* and in any subsequent normative act that shall replace this Emergency Ordinance.

**(2)** Accordingly, the Bank shall not be liable for any loss or damage of any nature whatsoever (including moral) incurred directly or indirectly by the Customer or third parties as a result of compliance with these regulations, arising from: **(i)** late execution/non-execution by the Bank of any payment instruction of the Customer **(ii)** blocking/closing of the Account/payment instruments; **(iii)** termination of the Specific Contracts.

**4.9.3.** The Client will be liable to the Bank for any loss suffered by it, as a result of not knowing to the Bank any restrictions or limitations regarding the Client / Account.

**4.9.4.** If the Client presents the Bank with payment orders or any other payment instruments that are false or potentially fraudulent in the Bank's sole discretion, causing payment risks, including those instruments that may affect the finality of settlement, they shall be subject to the legal sanctions provided for by the regulations in force, the Bank reserving the right not to execute the Client's Payment Order in these situations, without being held liable for any direct or indirect damage caused to the Client as a result.

**4.9.5.** The client is obliged to comply with the security requirements mentioned in the Specific Agreement regarding the payment operations.

**4.9.6.** The client has the obligation to notify the Bank as soon as he is aware of the loss, theft, the unauthorized use of the payment instrument or of any other unauthorized use of it, through the means of communication identified in the specific Contract, which are operational 24/7.

**4.9.7** In case of suspicion of fraud or real fraud or in the case of security threats, the Bank will notify the Client, being able to choose, depending on the situation, one or more of the following communication channels: SMS, voice call through the service by Call Center, by notification in the Smart Mobile or message transmitted to the e-mail address communicated to the Bank.

**4.9.8** The Bank has the right to block the use of the payment instrument in the cases and in compliance with the procedures agreed in the Specific Agreement.

**4.9.9.** In the event that there is reasonable suspicion of fraud or suspicion of unauthorized use by the Client or a third party of mobile banking/ Cards or any payment instrument or for reasons related to the security of the payment instrument. The Bank may suspend the Client's access to these services/payment instruments at any time, for a specific period of time. As a measure to protect the Client's interests in case of reasonable suspicion of fraud, the Bank may block the Client's access to the Account and/or access mobile banking/Cards services or through any channel, as well as any payment transactions carried out on the Client's Account, including transactions initiated through third party service providers (without the Client's prior consent, until any suspicion is removed, with notification to the Client of the measure taken, in accordance with the provisions of section 8. 2. "Notifications" or as provided in the specific Contract. In this respect, the Bank shall not be held liable for the non-execution and/or blocking of transactions ordered by the Client.

**4.9.10.** If the Bank finds that a Client's Account has been credited or is to be credited with amounts from other Clients'/other sources' accounts as a result of the Client's or third parties' allegedly illegal activities or in the event of suspected fraud, The Bank shall have the right, but shall not be obliged, to block and/or debit the Account of the Client who is the beneficiary of the payment at any time with the amounts resulting from the allegedly illegal activities with which the Client has been credited, without being held liable in any situation for any damages that the Client may suffer. The Bank shall notify the Customer of the action taken in accordance with the provisions of section 8.2.

#### **4.10. Unauthorized payment transactions, not executed or incorrectly executed. Liability of the parties**

**4.10.1** The client shall bear all losses related to any unauthorized payment transaction if such losses result from fraud or non-compliance, intentionally or through gross negligence, of one or more obligations related to the payment instrument, which are incurred, in accordance with the provisions of these GBC and of the legal regulations in force. Exceptions are the situations expressly provided by the legislation in force.

**4.10.2.** If the Client has notified the Bank of the loss, theft or unauthorized use of the payment instrument, he shall continue to be liable for the losses arising even after the Bank's notification, if he himself acted fraudulently.

**4.10.3.** The bank responds if the following conditions are cumulatively fulfilled:

- a) in the case of the payment operations not authorized by the Client and of the payment operations not executed or executed incorrectly by the Bank;
- b) if the amounts of money have not reached the Service Provider of the payment beneficiary, in case of operations not executed or executed incorrectly by the Bank.

**4.10.4.** In the case of an unauthorized payment operation, not executed or executed incorrectly, the Bank will proceed according to the law.

**4.10.5** If, as a result of the application of the legal provisions and of the provisions of this point 4.10, the Customer has been returned the amount related to a payment operation, both by the Bank and by the payment beneficiary or its payment service provider, the Bank is authorized to recover the entire amount returned to the

Customer, by debiting, at any time, the Account or with the respective amount, carrying out possible currency exchanges under the conditions of these GBC, without any previous notification or formality.

**4.10.6** The Bank is entitled to recover the amount/sums with which the Client has compensated for the Unauthorized, unexecuted or incorrectly executed payment operations in the event that the Client's fraud or the failure with his intention or gross negligence of the obligations incurred are subsequently proven or if it is found that the payment operation was executed incorrectly due to the Client's error. For the purpose of recovery, the Bank is authorized by the Client to debit at any time the Account or the amount with which it was compensated, carrying out possible currency exchanges under the conditions of these GBC, without any previous notification or formality.

**4.10.7.** The Bank corrects a payment operation only if the Client has notified the Bank within 30 days from the date of issuing the statement of account, but not later than 13 months, from the date of debiting the account, that it has found an unauthorized or incorrectly executed payment operation, which gives rise to a complaint. In case the Client informs the Bank of an Unauthorized or erroneous payment operation performed after 30 days from the date of issuing the statement of account, the Client is obliged to motivate the delay in reporting the respective operation.

**4.10.8.** The Bank, as a payment service provider of the Paying Client, makes, at his request, immediate efforts to identify and monitor the payment operation and to notify the Payer of the results, in the event of a non-executed payment operation or incorrectly executed in which the payment order is initiated by the Payer.

**4.10.9.** If the Bank is the payment service provider of the Payment Beneficiary and received the amount related to a payment operation executed incorrectly by the Payment Service Provider of the Payer, the Bank will credit this amount immediately to the Payee Beneficiary's account.

**4.10.10** The Bank shall not be liable for those payment transactions ordered by the Client which cannot be processed or processed late due to: lack of availability in the payment account, completion errors, illegality of transactions, malfunctions or limitations of systems owned or managed by third parties (other payment service providers, merchants, card acceptors, telephone service providers, internet service providers etc.), non-compliance with the conditions on payment orders imposed on the Bank by the NBR, correspondent banks and/or other authorized institutions, impossibility to read the information filled in the payment forms, execution of enforceable orders of the judicial bodies, lack of supporting documents related to the operation (in case the legal provisions require the presentation of such documents or the Bank has expressly requested such documents or in additional verifications according to the provisions of the present GBC) or in any other cases beyond the Bank's control and/or as a result of the verifications that the Bank must carry out, in order to comply with the legislation in force on the prevention and combating of money laundering, terrorist financing, fraud and for compliance with international sanctions regimes as well as for compliance with any other applicable regulations.

**4.10.11.** In case the unique identification code of the payment transaction provided by the Client is incorrect, the Bank is exempted from liability for non-execution or defective execution of the payment operation; The Bank will make reasonable efforts to recover the funds involved, receiving for this service a commission under the Specific Agreement.

**4.10.12.** The Bank shall not be held liable for any loss or damage of any kind incurred directly or indirectly by the Client as a result of the Bank's execution of any instructions of the Client, being accepted by both Parties that any instructions are given to the Bank by the Client at its risk and under its full responsibility.

**4.10.13.** The Bank will not be held liable for losses or damages of any kind incurred directly or indirectly by the Client by delaying the execution / non-execution by the Bank of any instructions of the Client following the compliance of the Bank with specific national or international legal regulations or of measures imposed by authorized bodies.

#### **4.11. Incorrect crediting**

**4.11.1** If a Client Account is mistakenly credited with an amount, the Client will retain that amount as an agent for the Bank and will not have the right to withdraw, transfer, dispose or use in any other way that amount in whole or in part. As soon as it becomes aware of any such incorrect credit, the Client will notify the Bank, and the Bank will have the right to debit the respective Account with any incorrectly credited amount.

**4.11.2** If, in breach of the obligation stipulated in point 4.11.1, the Client withdraws, transfers, disposes or uses in any way the incorrectly credited amount or part of it, the Client undertakes to repay immediately the Bank the respective amount and to compensate the Bank for any loss suffered as a result of this fact.

In this context, the Bank may proceed according to the section Discovered by an unauthorized account in these GBC, in which case the Bank's simple decision to debit the Account with the incorrectly credited amount that will exceed its credit balance has the legal value of early acceptance by the Customer of a non-revolving overdraft facility.

**4.11.3** If the crediting error is notified by the Bank, by the payment authorizing officer/payer's bank, the Bank has the right, without needing the notification or obtaining a prior authorization from the Client, to correct the error by debiting the account with the respective amount, based on documents in form and substance satisfactory to the Bank.

**4.11.4** The bank will inform the Client of the correction thus made through the statement of account.

**4.11.5** The Bank shall not be held liable for any loss or damage of any kind incurred directly or indirectly by the Client as a result of the Bank executing an instruction which subsequently proves to be transmitted by a person without quality / right, if the Bank proves that showed diligence, but the lack of quality / right / identity of the person who transmitted the instruction could only be established by special technical means and procedures.

## **5. CONTRACTUAL PROVISIONS RELATING TO THE ISSUE AND USE OF THE CARD**

### **5.1 Issuing Cards**

**5.1.1** The Bank offers its Clients debit cards attached to current accounts in Lei and/or foreign currency and credit cards.

**5.1.2 (1)** Debit cards are payment instruments attached to Current Accounts in lei or in EURO and USD.

**(2)** Credit cards are payment instruments attached to a credit line in lei granted by the Bank.

**(3)** The virtual card is a card issued exclusively on digital medium that allows transactions on the Internet and at Terminals. In order to carry out transactions at Terminals, the card must be previously registered in eWallets. The virtual card can be viewed and registered in eWallets exclusively through the Smart Mobile application.

**5.1.3** The cards can be used in the physical environment (applicable for embossed cards) and in the electronic environment (applicable for flat, embossed cards and virtual cards), in Romania and abroad.

**5.1.4. (1)** At the request of the Current Account holder, opened in one of the following currencies: Lei, Euro or USD, the Bank may attach main and/or additional Debit Cards. Regardless of the number of Current Accounts opened in a currency (Lei, Euro, USD), the Bank may attach to the Current Account a maximum of 2 (two) main Debit Cards and 2 (two) additional Debit Cards for each currency.

The Current Account holder's portfolio may contain a maximum of 2 (two) active primary debit cards and 2 (two) active supplementary debit cards for each currency at the same time. **(2)** For the Credit Card Account, at the request of the Cardholder, the Bank may issue one main Credit Card and a maximum of four (4) additional Credit Cards.

**(3)** The Bank may restrict the number of new Cards and reissued Cards, at the Customer's request, within a period of 30 days.

The number of new or reissued Cards that may be requested by the Customer is specified on the Bank's website [www.raiffeisen.ro](http://www.raiffeisen.ro) in the "In your support" section. The Bank reserves the right to change at any time the number of new/reissued Cards specified in the previous paragraph, informing card users by publishing specific information on the Bank's website, in the section mentioned above.

**5.1.5 (1)** The Bank shall deliver the Debit Card/Credit Card issued on a physical medium (upon first issue, upon automatic renewal upon expiry of the validity or upon reissue of the Card at the Client's request) to the mailing or home address in Romania, communicated by the Client to the Bank or at the address established in accordance with the provisions of point 8.2.4 of this document.

The Card User will be informed about the transmission of the Card by SMS to the telephone number communicated to the Bank or by push notification through the Smart Mobile application. If the Card cannot be returned to the Card User, it shall be returned to the Bank and handed over to the Customer in accordance with the details in paragraph (2).

(2) By exception, in certain situations (such as but not limited to: the Card User's identification and correspondence data are not updated, the Card User has not communicated a mobile phone number in Romania, the address communicated to the Bank is not in Romania), the Bank may establish another way of transmitting the Card to the Card User, and the Card User shall be informed on how to take possession of the Card, by SMS or by specific forms provided by the Bank. **5.1.6 (1)** The activation of the Card issued on a physical medium is performed by the Card User at the first POS/ATM/MFM transaction by inserting the Card into the terminal and entering the PIN code. PIN codes are communicated to the Card User by SMS message to the last mobile phone number declared to the Bank at the most recent data update made by the Card User. The Parties agree that after the Card is handed over, the Bank may send messages to the Client, through any channel, regarding the activation of this payment instrument.

(2) All Cards issued on a physical medium by the Bank have contactless technology incorporated, so that they can be used either by inserting the Card in the Payment Terminal or by approaching it, communication being carried out via radio waves. The Client may request the Bank to deactivate the contactless functionality of the Card at any of the Bank's branches or through the Call Centre Service and is obliged to comply with the deactivation procedure communicated to him/her upon request.

**5.1.7** The Card is and remains permanently the property of the Bank. Card Users have the right to use the Cards and are obliged to return them at the Bank's request.

**5.1.8** The use of the Card is only allowed to the User who has his/her name on the Card.

By exception, for certain types of debit/credit cards, the Bank offers the possibility for the Account Holder to request the issuance (provision) of a Card in the Bank's branches, immediately after approval of his/her application, in which case a generic name (e.g. "Instant Card") will be written on the Card instead of the name of the main or additional Card User. On reissue/renewal, these Cards will be personalised with the Card User's name.

**5.1.9** The Card is non-transferable and may only be used within the time limit specified on the front of the Card and in accordance with the provisions on the use of the Card in this section; Debit Cards, including additional debit cards, may be registered by the Bank with the IBAN code belonging to the Current Account to which such cards are attached.

**5.1.10** The Bank will automatically renew the Card at any time during the last 45 calendar days of the Card's validity, except in situations where the User notifies the Bank 45 calendar days prior to the expiry of the Card of his/her intention to waive renewal or in situations where the Debit Card is attached to a dormant or closed Current Account at the time of renewal;

## **5.2 Provisions for Additional Users**

**5.2.1.** The Current Account/Credit Card Holder may choose to grant access to the amounts in his/her Account to additional Card User(s), provided that such individual is of full age, in full possession of his/her civil rights and, if applicable, completes and signs, together with the Account Holder, the forms provided by the Bank.

**5.2.2.** The Additional Card User has the right to dispose of the amounts in the Account Holder's account under the same conditions as the Account Holder, and, if applicable, in compliance with the limits on the use of amounts imposed by the Primary Card User, without however having the right to receive statements of account/activity reports which highlight the operations carried out through the Cards (Primary and Additional), to initiate transfers from the account without using the Card, to close/modify the current/card account, to surrender or request modification of the credit line attached to the Card account. The Supplementary Debit Card User may request the closure of the Card issued in his/her name.

**5.2.3.** The Additional Card shall be handed over to the Account Holder and/or the Additional User.

**5.2.4.** The Additional User will be able **(i)** to consult, using the Debit Card in his/her possession, the funds available on the current account and, in the case of the Credit Card, the funds available on his/her Card; **(ii)** to dispute only the transactions carried out with his/her Additional Card; **(iii)** to obtain a mini statement of account, **(iv)** to register the Card in eWallets.

**5.2.5** The Primary Card User understands and agrees that the Additional Card User may register the Additional Card issued in his/her name in one or more eWallets and assumes the methods of registration and authorization of payments and all transactions made through the eWallet by the Additional Card User.

**5.2.6** The Bank may refuse Additional Users appointed by the Primary Card User, on or after the date of appointment, if there are suspicions or reasonable grounds for suspicion of money laundering, terrorist financing, fraud, International/US Sanctions or in any other situation where legal regulations so require. The Bank will not accept Designated Persons or Restricted Parties as additional Users. If the Bank rejects existing Additional Users, it will notify the Customer in writing of the date from which the Additional User is no longer accepted by the Bank.

### 5.3 Use of Cards

**5.3.1.** As a rule, the Customer expresses his/her consent to authorize Card Payment Transactions through Strict Customer Authentication, under the conditions and with the application of the exceptions provided for by the Romanian legislation and European regulations.

**5.3.2** Payment transactions ordered by means of the Card shall be deemed authorized by the Card User if he/she has given his/her consent by using the security features, as follows:

**a) for ATM/MFM transactions:** using the Card and PIN. In case of using an eWallet, the transaction is carried out by approaching the mobile device with payment function to the contactless terminal (ATM/MFM), unlocking, if necessary, the mobile device and then continuing the transaction on the Payment Terminal screen, including entering the PIN of the eWallet.

**b) for point of sale transactions ("EPOS"):** usually by inserting or bringing the Card close to the EPOS, entering the PIN code and/or signing the receipt generated by the EPOS; In the case of **Small Value Card Payments**, the payment authorization is performed as described in **5.3.4** below without the need to sign the receipt issued by the EPOS and/or enter the PIN code.

**c) for transactions at Imprinter:** by using the Card and the signature on the receipt generated by the payment terminal.

**d) for e-commerce transactions:**

**(i) in the case of sites not enrolled in the 3-D SECURE Service:** payment authorization is made by providing the data entered on the Card, under the terms and conditions agreed by the Card User with the merchant;

**(ii) in the case of sites enrolled in the 3-D SECURE Electronic Commerce Service,** the payment authorization is made through the Customer's Strict Authentication, being necessary to provide the security elements specific to this type of authorization, mentioned in the Terms and Conditions specific to the use of this service, provided in paragraph **5.8** below;

**(iii) in the case of Small Value Card Payments,** the authorization of the payment shall be made in accordance with the provisions of paragraph **5.3.4** of the CGB.

**e) for transactions without a Card present, by post or telephone (MOTO transactions):** by providing the merchant with some of the data entered on the Card, in order for the merchant to initiate payments according to the terms and conditions agreed with the merchant as the beneficiary of the payment.

**f) for transactions carried out with the use of the Card for small amounts, at unattended terminals** (e.g. motorway tolls, parking fees, etc.): by using the Card and reading the information from the Card's CIP

**g) for transactions carried out via the Card using technologies, software applications and/or mobile devices (e.g. eWallet):** by using the security features regulated in the specific terms and conditions of the software applications/mobile devices.

**5.3.3** Certain types of Card Transactions in e-commerce, by exception to the provisions of **5.3.2 (d) (ii)**, may be authorised by the Card User as follows:

**(i) Recurring Transactions** (a series of payments of the same amount made to the same payee at certain intervals of time e.g. monthly, weekly etc.) - the Card User authorises the first payment transaction through Strict Customer Authorisation and subsequent payments in the series are deemed to be authorised by the Card User, without providing the security features associated with Strict Customer Authentication;

**(ii) Transactions for which the Card User has given the payee/merchant a mandate on the Card User's website to initiate payments on his/her behalf** - the Card User provides the security elements of the Strict Customer Authentication at the time of giving the mandate to the payee/merchant and the payments are initiated by the payee/merchant without the Card User applying the Strict Customer Authorisation;

(iii) Electronic transactions identified as low risk - authorization of these transactions is done by providing the data entered on the Card, without the introduction of security elements related to Strict Customer Authentication. The low level of risk is determined, according to legal provisions, from the analysis of the Card User's transaction profile, taking into account several parameters such as, but not limited to, the amount and currency of transactions, the merchant's country, repeated transactions to an agreed beneficiary, performing transactions from the same device.

**5.3.4** For Small Value Card Payments authorised using contactless technology and/or over the internet (e-commerce) the Card User is deemed to have given his/her consent to the payment transaction by simply bringing the Card/mobile device with payment function close to an EPOS/ATM/MFM Terminal or by providing card data for internet transactions (e-commerce), without the need for Strict Customer Authentication, if the cumulative amount or the cumulative number of Small Value Payments made since the last application of Strict Customer Authentication, as determined by the Bank/International Card Organizations and published on the Raiffeisen Bank website, is met.ro. The value of these limits may be modified by regulatory acts and/or by the international card organisations, and the Client will be informed accordingly on the Bank's website/agencies of the new limits. The limit may not be higher than the limit established by law.

**5.3.5 (1)** The Bank has the right to set certain transaction limits (such as but not limited to: maximum daily number of transactions, daily cash withdrawal/transaction limit) through the Card (both for the Primary Card and the Supplementary Card), which limits are indicated in the Specific Agreement and/or in the Specific Lists and/or on the Bank's website.

**(2)** The Bank reserves the right to modify at any time the limits provided for in the previous paragraph or to restrict certain types of transactions with the Card, informing Card Users by publishing specific information on the Bank's website [www.raiffeisen.ro](http://www.raiffeisen.ro) in the "In your support" section.

**(3)** For security reasons, the Visa card organization may impose certain restrictions on transactions made with the Card, such as exceeding a certain number or value of transactions. The Bank cannot be held liable to the paying or beneficiary Customer for any direct or indirect damages resulting from the rejection of Transactions by the Visa card organization, given that the limits and rejection of transactions are set at the Visa system level.

**5.3.6** The Bank is authorized by the Primary Card User to automatically debit the following amounts from the current/card account:

- a) transactions/transactions carried out by Card in the country and abroad, by the Primary User and Additional Users;
- b) other operations expressly ordered by the Primary Card User;
- c) fees, charges and interest due to the Bank for current operations, issuing/replacing Cards and/or for special services under the Specific Agreement;
- d) fraudulent operations carried out by persons other than the Card User in the event of loss/theft of the Card and failure to notify the Bank, by telephone or in writing, of the event by the main or additional Card Users in compliance with the limits established by law;
- e) fees paid by the Bank for the resolution of disputes by the Primary Card User;
- f) interest owed by the Primary Cardholder on amounts that have generated unauthorised overdrafts on the current account, i.e., in the case of the Credit Card, costs related to the Credit Card and interest owed to the Bank on amounts used from the Credit Limit related to the Card.

**5.3.7** As a rule, Transactions are made within the limits of the available funds in the Cardholder's current/credit card account. Exceptionally, the Bank may execute the Payment Transaction in the situations described in **5.3.8** below;

**5.3.8** Accidental overdraft of the available funds in the Current Account with the Card attached may occur due to the debiting of the Current Account with the interest due to the Bank by the Account Holder, with the counter value of the Payment Transactions ordered on the Current Account, with fees and/or commissions related to the Current Account and/or to the use of the Card, or due to malfunctions of the communication systems owned or managed by third parties (banks, merchants, card acceptors, telephone service providers, etc.), in the case of offline payments or small value Card payments, using contactless technology, for which no availability check was requested at the time of transaction authorisation, and the transaction authorisation was not carried out with PIN request and/or receipt signature.

**5.3.9** In case of unauthorized overdraft of the Current Account, the provisions of section 3.4 of these GTC shall apply; the Bank may also decide to block access to the Current Account/Card via all Cards attached to it.

**5.3.10** The Card User will be able to obtain at Raiffeisen Bank ATM/MFM Terminals a mini-account statement, containing the last 10 transactions made in connection with the current account with the attached Debit Card, regardless of the applicant or the payment channel/instrument through which they were made.

#### **5.4 Making payments via Cards**

**5.4.1** Once a Card Transaction has been authorised, it is irrevocable and is carried out in real time, the Account being blocked with the countervalue of the Card Transaction at the time it is carried out. The settlement of the amount blocked at the time of authorisation of the Card Transaction in the card acceptance networks will be carried out within the deadlines set by the international card organisations.

**5.4.2** In certain limited situations, Card Transactions may also be carried out off-line, in which case the transaction is sent directly for settlement, without the transaction amount having been previously blocked on the Account. Both the blocking of the Card Transaction amount and its settlement are carried out automatically by the payment system, without the bank being able to intervene in the commercial relations between customers and merchants/accepting banks.

**5.4.3** For Card Transactions made in the currency of the Account, carried out by means of Visa Cards attached to accounts opened in Lei, Euro, USD, the Bank shall record in the current Account attached to the Card the amount related to the Card Transaction (debit/credit of the Account), without currency conversion.

**5.4.4** Visa transactions made in a currency other than the currency of the Account shall be recorded in the Account attached to the Card by performing a currency conversion, using the Euro as the reference currency, as follows: **(a)** the currency exchange between the currency in which the Transaction is carried out and the Euro is performed by the Visa International organization at its domestic rate on the settlement date; **(b)** for the conversion of the Transaction amount from the Euro into the currency of the Client's Account, the Bank uses the Bank's Exchange Rate for Card Transactions, valid for the date of posting the Transaction to the Account.

**5.4.5 (1)** As an exception to paragraph **5.4.4**, Visa Transactions attached to Accounts opened in USD, carried out in a currency other than that of the Account, except for transactions in Lei carried out in Romania, shall be recorded in the Account using the USD as the reference currency. The currency exchange between the currency in which the Card Transaction is carried out and the reference currency shall be carried out by Visa International at its domestic rate on the date of settlement of the Card Transaction increased by the Currency conversion fee; **(2)** Card Transactions made in lei on the territory of Romania by Visa cards attached to accounts opened in USD, shall be recorded in the Account with the value of the Card Transaction by making the exchange between the currency of the transaction and the currency of the Account, using the Bank's exchange rate for Card Transactions valid for the date of posting the transaction on the Account.

**5.4.6 (1)** As an exception to paragraph **5.4.4**, Visa Card Transactions attached to accounts opened in Euro, carried out in a currency other than that of the Account, with the exception of transactions in Lei carried out on the territory of Romania, shall be recorded in the Account using Euro as the reference currency. The currency exchange between the currency in which the Card Transaction is carried out and the reference currency shall be carried out by Visa International at its domestic exchange rate on the settlement date of the Card Transaction increased by the Currency conversion fee;

**(2)** Transactions by Visa Cards attached to accounts opened in Euro, carried out in lei on the territory of Romania, shall be recorded in the Account by making the exchange between the currency of the transaction and the currency of the Account, using the Bank's Exchange Rate for Card Transactions valid for the Transaction Posting Date on the Account.

**5.4.7** Card transactions carried out at the Bank's Terminals in a currency other than the currency of the Account shall be recorded on the Account by performing the currency conversion as follows:

**(i)** For Card Transactions in USD made through Cards attached to Accounts opened in Euro, the currency conversion shall be performed using the Leu as reference currency, as follows: **(a)** the currency exchange between USD and Leu shall be performed by applying the Bank's Exchange Rate for Card Transactions valid on the date of posting of the Card Transaction on the Account; **(b)** the currency exchange between Lei and Euro shall be performed by applying the Bank's Exchange Rate for Card Transactions valid on the date of posting of the Card Transaction on the Account.

(ii) For Card Transactions in USD made through Cards attached to accounts opened in Lei, the currency conversion between the transaction currency and the Account currency shall be performed by applying the Exchange Rate for Card Transactions valid for the date of posting the Card Transaction on the Account.

(iii) For Card Transactions in Euro carried out through Cards attached to accounts opened in USD, the currency conversion shall be performed using the Leu as reference currency, as follows: (a) the currency exchange between Euro and Lei shall be performed by applying the Bank's Exchange Rate for Card Transactions valid on the date of posting the Card Transaction on the Account; (b) the currency exchange between Lei and USD shall be performed by applying the Bank's Exchange Rate for Card Transactions valid on the date of posting the Card Transaction on the Account.

(iv) For Card Transactions in Euro carried out through Cards attached to accounts opened in Lei, the currency conversion between the transaction currency and the Account currency shall be performed by applying the Bank's Exchange Rate for Card Transactions valid on the date of posting the Card Transaction on the Account.

**5.4.8** The exchange rates used by the Visa International organisation can be found on the websites of this organisation.

The Bank's exchange rate for Card Transactions and the Currency conversion fee are displayed on the Bank's website, [raiffeisen.ro](http://raiffeisen.ro).

**5.4.9** The Bank shall ensure transparency and comparability of currency conversion fees when the Card User makes cash withdrawal transactions at an ATM/MFM or payments at EPOS within the European Union (EU). Thus, for these transactions made in Euro or in a national currency of an EU Member State other than the currency of the Account, the Bank will display on its website [www.raiffeisen.ro](http://www.raiffeisen.ro) the total amount of the foreign exchange fees expressed as a margin added to the latest Euro reference exchange rates published by the European Central Bank (ECB).

**5.4.10** In addition, the Bank will send an electronic notification to the Cardholder each month after it receives from the Cardholder a Payment Order for a transaction of the type referred to in point **5.4.9**.

**5.4.11** The Bank and the Card User agree that the Bank shall send the electronic notification containing the applied exchange rate, expressed as a margin added to the latest Euro reference exchange rates published by the ECB by: (i) push notification on the Customer's mobile device, for Customers who have the Smart Mobile Service; (ii) electronic notification sent by e-mail/SMS to the e-mail address/mobile phone number communicated to the Bank, for Customers who do not have the mobile banking service offered by the Bank;

**5.4.12** The Card User may at any time request the Bank to stop sending him/her the electronic notifications mentioned in the previous paragraph, through the Call Center Service for Customers receiving SMS notifications or by deactivating the push notifications within the Smart Mobile application, by Customers receiving push notifications.

## **5.5. Rights and obligations of the parties regarding the Card**

**5.5.1** Card Users are obliged to ensure by all means the security of the Card, PIN, Static Password and eWallet security features.

**5.5.2** Card users have the obligation:

**a)** to sign the Card issued on a physical medium on the reverse side in the box reserved for this purpose, at the time of its receipt, using a ballpoint pen with paste;

**b)** to keep the Card carefully and not to disclose specific identification information (card number, expiry date, authentication codes, etc.) to other persons;

**c)** not to lend the Card to other persons;

**d)** ensure that during transactions the Card remains under their close supervision;

**e)** before deleting the SMS message, they must memorize or write down the PIN in a place known only to them;

**f)** never write the PIN on the Card or in a form that can be easily recognised in private or on an object accessible to other persons;

**g)** not to reveal to any other person the PIN, the Static Password used for e-commerce transactions, even if he/she is or presents himself/herself as an employee of the Bank; also the PIN code must not be entered on Internet sites;

**h)** ensure that, during transactions carried out using the PIN, it is not disclosed voluntarily or involuntarily to other persons.

i) not to provide any data related to the Card (card number, expiry date, the string of the last 3 digits written on the back of the card in the space provided for the User's signature and/or PIN), OTP code or Static Password by replying to e-mails in which they are requested to do so; Raiffeisen Bank will never request such information by e-mail;

j) to maintain the confidentiality of data and information that may constitute an element of identification in the relationship with the Bank.

k) to change at any Raiffeisen Bank ATM/MFM or any ATM in Romania, the initial PIN received by SMS.

**5.5.3** In case of loss/theft of the Card or PIN, the Primary/Supplementary Card User is obliged to notify the Bank by telephone through the Call Center Service provided or by using the assistance numbers printed on the Card or by a written notification to block access to the Account through the Card or for users of mobile banking service to block the Card directly from the application related to the service. The written notification shall be submitted to any territorial unit of the Bank during working hours with the public. The parties shall be liable for the transactions carried out with the Card in accordance with the clauses set out in section **4.10** of these GTC.

**5.5.4** The Card User shall also notify the Bank in writing at any banking establishment and/or by telephone through the Call Center service as soon as he/she notices one of the following emergency situations:

- a) damage or blocking of the possibility to use the Card (e.g. capture of the Card in the ATM);
- b) recording transactions in the Current/Credit Card Account that have not been ordered by the Card Users;
- c) any entry in the Current/Credit Card Account which, in its opinion, represents an erroneous entry arising from the Bank's management of the Account;
- d) there are elements that create suspicions about the possibility of knowledge by persons other than the Card User;

e) Card malfunctions or incorrect PIN/access password received;

f) loss/theft of the mobile device on which an eWallet is installed or compromise of any of their security features.

**5.5.5 (1)** If the Card User uses the services provided by merchants that allow saving/recording of card data to make subsequent payments on the websites or in the applications of those merchants, the Card User assumes the following obligations and declarations:

a) He/she shall ensure that he/she complies with all obligations incumbent upon him/her under these contractual provisions throughout the use of the services offered by the trader;

b) Understands that in order to access these services it is necessary to enter on the merchant's website/application the data of the Card he/she wishes to save for future payments, namely: Card number, Card expiry date, CVV code and understands that the Bank will respond to any requests from payment scheme Visato validate these data that it holds by virtue of its capacity as Card issuer, as well as provide them with information regarding Card replacement;

c) Understands and accepts that in case of renewal or reissue of the Card whose data has been saved/registered on the merchant's website/application, the new expiry date of the renewed/issued Card will be automatically updated on the merchant's website/application (except for the hypothesis provided for in letter d)); in the event that the updates are not desired, the Card User is obliged to access the merchant's website/application and delete the Card data from his/her records. In case the merchant does not offer the possibility or does not respond to the request for deletion of the saved Card, the Card User shall contact the Bank, requesting the closure of the respective Card and the issuance of a new Card with a different Card number than the closed one;

d) Understands and accepts that, in the event that the Card whose data was saved/registered on the Merchant's website/application has been replaced/issued due to reported loss, theft or fraud, the original Card will be inactivated and the reissued Card data will not be automatically updated at the Merchant, but will have to be saved/registered again in order to be used for making payments on the Merchant's website/application;

**(2)** In the relationship with the Bank, the Card User is responsible for all consequences arising from his/her choice to use such services provided by merchants. As the Bank is a third party to the relationship established between the Card User and the Merchant, the Bank shall not be liable for any services provided to the Card User by the Merchant and shall not be held liable for any consequences resulting directly or indirectly from the Card User's use of such services provided by the Merchant.

**(3)** The provisions of **paragraph 2.1** of the CGB are applicable with regard to other aspects of processing of personal data.

**5.5.6** The Bank shall have no liability in respect of non-acceptance of Cards by a merchant, financial institution, ATM/MFM or any other third party as a result of any direct or indirect cause, such as: failure of the machine, processing or data transmission system or any other events beyond the Bank's control.

**5.5.7** Use of the Card is prohibited:

- a) after the Bank has been notified of the loss/theft of the Card/ or PIN;
- b) when the Card User has breached the contractual provisions and the Bank has requested the return of the Card;
- c) when a Card reported lost or stolen is recovered by the Primary/Supplementary Card User after the Bank has been notified of the loss/theft;
- d) when a Debit Card is cancelled or blocked by the Bank due to accidental overdraft and non-payment of the Current Account;
- e) when a Credit Card is cancelled or suspended by the Bank due to the Primary Card User's failure to comply with the repayment discipline of the amounts used from the credit limit attached to the Credit Card Account;

## **5.6. Blocking Cards**

**5.6.1** The Bank reserves the right to block the Card without prior notice to the User in the event of the User providing false data in the documentation submitted to the Bank, committing fraud if the Bank has identified suspicions of fraud/money laundering/terrorist financing/infringement of International/US Sanctions, in situations in which the Client has received requests for the return of funds from the ordering/corresponding banks for the reasons listed above, or in situations in which the Bank has received information on suspicions of fraud/money laundering/terrorist financing/international sanctions/USA infringement against the Client from banks or authorities in Romania or abroad, or in any other situation considered justified by the Bank.

**5.6.2** For situations other than those mentioned above, the Bank shall inform the Client via the Call Center/SMS telephone service of the blocking of the Card and the reasons for such blocking immediately after the blocking, unless the provision of such information is contrary to justified safety reasons or is prohibited by other legal provisions.

## **5.7 Challenging Card transactions**

**5.7.1** In the event that the Card User finds that transactions not authorized by the Card User have been carried out, the Primary Card User has the right to dispute any such transactions. The Additional Card User will only be able to lodge disputes for transactions carried out with his/her Additional Card.

**5.7.2** The dispute shall be submitted in writing to any Bank unit during working hours with the public and/or by telephone through the Call Center service and shall include the card number, the name of the Card User, the disputed amount, the date of the statement containing the disputed amount and any additional information supporting the dispute.

**5.7.3** The Bank shall inform the Card User in writing or by telephone, in compliance with the legal provisions, on how to resolve the dispute.

## **5.8 Terms and conditions specific to the use of the Card in the 3-D SECURE e-commerce service**

**5.8.1** All cards issued by Raiffeisen Bank are enrolled in the 3-D Secure Electronic Commerce service, which ensures the security of e-commerce transactions carried out via the Internet under strict security conditions, in accordance with the provisions of these clauses.

**5.8.2** The Bank may periodically modify the instructions for use of this service in accordance with the law. The parties agree that the Card User's silence shall constitute tacit acceptance of the changes if the Card User does not notify the Bank in writing of his non-acceptance of the changes before they come into force.

The latest version of the instructions is available on the Raiffeisen Bank website, [www.raiffeisen.ro](http://www.raiffeisen.ro).

Transactions carried out using the 3-D Secure eCommerce service are subject to the latest version of the Terms and Conditions of Use.

**5.8.3** The 3-D Secure eCommerce Service is provided by Raiffeisen Bank through a processor with secure means provided by the respective card payment schemes, VISA International.

The 3-D Secure Electronic Commerce service works provided that the website where the transaction is performed supports 3-D Secure standards, featuring the logos displayed on the Bank's website, [www.raiffeisen.ro](http://www.raiffeisen.ro).

**5.8.4** Visa International reserves the right to modify, improve or discontinue the provision of this service without prior notice.

**5.8.5** The 3-D Secure e-Commerce service provides a standard of security for Internet transactions that incorporates the latest technologies in this field, reducing the chances of Internet fraud.

**5.8.6** Signing up for this service requires the provision of online data that will be used later to confirm the Customer's identity when performing transactions on the Internet.

**5.8.7** Authorization of 3D Secure transactions is achieved by applying Strict Customer Authentication, using one of the following methods:

a) for customers who do not have the Smart Mobile application, **by providing the following security elements:**

- **OTP (one time password):** a unique code associated with each transaction, provided to each individual Card User, either by SMS message to the personal telephone number declared to the Bank by the Card User in the most recent Enrolment/Update Form.

**and**

- **Static Password**

b) for customers who have the Smart Mobile application, **through the specific application provided by the Bank**, which allows authorization by biometrics or PIN according to the option set by the user in the application.

**5.8.8** The following are prohibited to the Card User:

- a) Intentionally substituting another person or entity to use the 3-D Secure Electronic Commerce service.
- b) Sending by any means virus-type programs that disrupt, destroy or limit the functionality of any hard/soft component, including communications of the accessed service.
- c) Sending unsolicited e-mails (spam), by any means, and hacking into the Verified by Visa and MasterCard Secure Code sites accessed.
- d) Modifying, adapting, decompiling or disassembling, sub-licensing, translating, selling any portion of the 3-D Secure Service.
- e) Deletion of any proprietary rights notices (copyright, trademark) obtained through access to this service.
- f) Using any means (search applications, devices, processes) to find or reproduce the navigation structure, presentation and content of websites displaying the specific Visa and MasterCard logos.
- g) Interrupting other users' access to this service, servers or networks connected to it.
- h) Violation of the specific rules and conditions of use of the 3-D Secure service in general and/or the rules and procedures of any network connected to it.

**5.8.9** Raiffeisen Bank and/or Visa International cannot be held liable for:

- a) modification, suspension or any interruption in the provision of the service due to causes beyond their control;
- b) malfunctions of the Card User's computer or in the provision of telephone services, occurring during Internet transactions;
- c) any damage caused by virus infection of the Card User's computer/modem during Internet transactions. Raiffeisen Bank reserves the right to temporarily or permanently disable the Card User's access to the 3D Secure service in case of violation of the terms of use.

The Bank will inform the Card User via the Call Center telephone service of the deactivation of the service and the reasons for this action immediately after it has been taken, unless the provision of this information is contrary to justified safety reasons or is prohibited by other legal provisions.

**5.8.10 (1)** The Card User has full freedom to purchase goods/services via the Internet by accessing the 3D Secure service. However, correspondence with the chosen merchants, participation in online promotions, payment and delivery of the goods/services purchased, any other conditions and guarantees associated therewith are solely within the scope of the relationship between the Card User and the virtual merchant, and Raiffeisen Bank or Visa International cannot be held liable in any way for any damages arising from the direct relationship with the merchants. The use of the service in no way implies that Raiffeisen Bank or Visa International recommends any internet merchant or that it guarantees the quality of the goods/services provided by the merchant.

(2) Any dispute regarding the merchant's failure to comply with the terms of payment, delivery, quality of goods/services purchased can be settled exclusively between the Card User and the merchant. In this regard, the Bank recommends that the Card User retains as much information as possible about the Merchant and saves on his/her computer or page the proof of the transaction.

**5.8.11** The 3-D Secure Service contains information protected by intellectual property and other applicable laws.

Raiffeisen Bank grants the Card User a non-exclusive license to use the current 3-D Secure service and enhancements that will be added over time in accordance with these terms. The Card User shall not copy, alter or use in any way the Raiffeisen trademarks owned by Raiffeisen Bank, 3-D Secure owned by Visa International and the logos, products and names associated with this service.

## **5.9. Registration and use of Cards in eWallets**

### **5.9.1 General conditions for the use of cards in electronic wallets**

**5.9.1.1** Eligible Cards issued by the Bank may be registered by Card Users in eWallets belonging to the Bank or other providers of such applications, by methods made available by them.

**5.9.1.2** Eligible Cards and mobile devices on which Cards can be registered are determined and communicated to the Card User by the Bank and/or the eWallet provider.

**5.9.1.3** The User has the possibility to add the same Card in several eWallets and on several devices with payment function at the same time. The mobile device provider may impose limitations or restrictions on the use of the eWallet and/or may have minimum software and hardware requirements for the compatible mobile device used. The User is obliged to use the Card only on a mobile device compatible with the eWallet functionality and to comply with all terms and conditions applicable to that eWallet.

**5.9.1.4** The provider of the eWallet and/or mobile payment devices with which payments can be made via the eWallet and third parties with whom they collaborate may have their own terms and conditions and privacy policies. The User is subject to the respective terms and conditions or privacy policies when using the eWallet/mobile device with payment function. The Bank assumes no responsibility for the way in which they use the information that the User makes available to them, nor for the User's personal data that they process in the context of the services they offer or when visiting their websites. Furthermore, the Bank is in no way responsible for the requirements of the eWallet/mobile device provider with payment function or of the third parties with whom they collaborate to impose conditions for the registration of the Card in the eWallet or concerning compatible mobile devices.

**5.9.1.5** The Bank has the right to block, restrict, suspend or terminate the possibility to use any Card enrolled in an eWallet if: **(i)** the Bank considers that the authentication and payment methods used by it are not sufficiently secure or do not comply with legal provisions; **(ii)** if it suspects any fraudulent or improper activity of the Card in the eWallet or in any other payment method; **(iii)** if the contractual clauses agreed with the Bank regarding the use of the Card are violated. The Bank also reserves the right to cease offering the possibility of using Cards in eWallets entirely.

**5.9.1.6** In the event that the provider of mobile devices with payment function and/or of the eWallet blocks, restricts, suspends or interrupts the use of the eWallet and/or changes its functionality, the Bank shall not be liable to its customers who have enrolled their Card in the eWallet or to third parties.

**5.9.1.7** The Card User is responsible for all uses and transactions made with the Card via the eWallet by third parties to whom he/she has given voluntary or involuntary access to the Card enrolled in the eWallet.

### **5.9.2. Card registration in the eWallet**

**5.9.2.1** The procedure for enrolling/registering the Card in the eWallet is determined by the provider of the eWallet. The Card User is obliged to set a password or other security details in order to use/access the eWallet. The conditions, cases and frequency with which this password will be required are set by the eWallet provider.

**5.9.2.2** After setting the password/security details, the User will be asked to enter the data of the Card he/she wishes to enroll in the eWallet, namely: card number, card expiry date, CVV code. All this information (personal data) is required by the eWallet provider in order to allow the card to be used for payment.

**5.9.2.3** In order to validate the identity of the Card User to be enrolled in the eWallet, the Bank will apply a customer authentication procedure. If the result of the procedure is positive, the Card may be enrolled in the Electronic Wallet.

**5.9.2.4** Following the registration of the Card in the eWallet, a payment token of the respective Card (alternative card number) will be generated, which will be associated to the Card on the mobile device with payment function; if there is the possibility, if the User wishes to register the Card on more than one mobile device, he will make the necessary settings in the eWallet, by adding the mobile devices on which he wishes to register the Card. The Token number is different from the number on the front of the Card registered in the eWallet for increased transaction security.

**5.9.2.5** By completing all the steps and completing the procedure for registering the Card in the eWallet, the User understands that the Card will be enrolled in the eWallet in order to be used to perform payment transactions and to view transactions made with the Card via the eWallet.

**5.9.2.6** The Bank may decide to refuse the request for registration of the Card in an Electronic Wallet. If the registration request is rejected, the User may contact the Bank's Call Centre Service for support.

**5.9.2.7** The registration and use of the Token depends on the eWallet provider and/or the Card User's internet provider network. The Bank has no direct or indirect control over the operations of these providers and shall not be liable for any situation related to the services provided by them that may cause interruption and/or prevention of the registration/use of the Token for making payments.

### **5.9.3. How the eWallet works**

#### **A) Making card payments via eWallet**

**5.9.3.1** Any of the following payment operations can be carried out using the eWallet:

- contactless payments with an enrolled Card, at Terminals with contactless function, via the compatible mobile device with payment function for which the card has been registered;
- internet payments to merchants (e-commerce and m-commerce)

**5.9.3.2** How the eWallet is used for making payments by the Card User and the security features used to authorise payments (mobile device unlock, application PIN, etc.) are established and communicated by the eWallet provider.

#### **B) View information and card payments in the eWallet**

**5.9.3.3** The Bank shall provide you with information about payments made with the card enrolled in the eWallet in the agreed ways (e.g. statement of account, mobile banking, etc.). This information will be highlighted as payments made with the respective Card, without indicating that the payments were made through the eWallet.

**5.9.3.4** If the eWallet allows it, the User will be able to view information about card payments made through the eWallet within the application.

#### **C) Suspension, replacement, renewal and deletion of the Card in the eWallet**

**5.9.3.5** The User has the possibility to suspend and/or temporarily/permanently block and/or delete one or all cards enrolled in the eWallet. Suspension, blocking, deletion, as well as the termination of suspension/blocking can be carried out directly within the eWallet, according to the Terms and Conditions communicated by the eWallet provider, or through the Bank's Call Centre Service. During the suspension/blocking period, the respective Card enrolled in the eWallet will no longer be able to be used to make payments via the associated mobile payment device.

**5.9.3.6** The suspension/blocking of the Card or deletion of Card data from the eWallet shall in no way affect the possibility of the Card to continue to be used for payments in accordance with the specific Debit/Credit Card Agreements as well as these PF GTC. All transactions made via the eWallet with the suspended/deleted Card prior to the time of suspension/deletion will be processed by the Bank in accordance with the provisions of the specific Agreements and the GTC.

**5.9.3.7** If the Card enrolled in the eWallet has been replaced/reissued due to reported loss, theft or fraud, the original Card will be inactivated in the eWallet and the reissued Card will have to be re-enrolled in order to be used for payments through the eWallet.

**5.9.3.8** If the card enrolled in the eWallet expires, the new card will need to be re-enrolled.

**5.9.3.9** If the Card User invalidates the password and/or security credentials for accessing the eWallet and/or the mobile device with payment function or if he/she resets the mobile device where the eWallet is downloaded or the mobile device used for payment with the Card, it is necessary to repeat the initial Card registration steps in case the User wishes to use the Card again via the eWallet.

### **5.9.4. Protecting the security credentials needed to use the eWallet**

**5.9.4.1** The Card User is responsible for maintaining the confidentiality of the security credentials required to use the eWallet. The Card User is also responsible for preventing fraudulent or unauthorised use of the Card via the eWallet or mobile payment device.

**5.9.4.2** If the User considers that the security credentials necessary for the use of the eWallet have been compromised (e.g. have become known to other persons), he/she is obliged to change them immediately.

**5.9.4.3** The Card User is obliged to contact the Bank immediately via the Call Centre Service in case:

- The card registered in the eWallet is lost or stolen or used without the User's consent;
- The mobile device used to access the eWallet and/or the mobile device with payment function associated with the card enrolled in the Wallet is lost, stolen or used without the User's consent;
- The security credentials required to use the eWallet have been compromised.

**5.9.4.4** All transactions with the Card carried out via the eWallet up to the moment when the Card User informs the Bank of the occurrence of one of the above mentioned events shall be considered as transactions authorized by the User, and the Bank shall not be liable for them. Furthermore, the Bank shall not be liable for the Card being used for payments via the eWallet on the basis of the Security Credentials, if these have been used by other persons, regardless of whether they have been communicated to them by the User or have been used in any way without the User's consent.

**5.9.4.5** In order to prevent the occurrence of events such as the above, the Card User undertakes:

- to keep the mobile device through which the eWallet is accessed and/or the mobile device with payment function associated with the card enrolled in the Wallet safe and in his/her possession at all times;
- to keep the Security Credentials for the use of the eWallet secure and known only to him/her;
- set different passwords/security details for the eWallet card than those used for the physical card;
- if they misappropriate or cease to use the mobile device through which the eWallet is accessed and/or the mobile device with payment function associated with the card enrolled in the eWallet, delete all cards and other personal information on it. For details on how to proceed in this case, follow the instructions of the eWallet provider.

**5.9.4.6** The User has the obligation to cooperate with the Bank and/or any competent authority for the prevention of any type of fraud or for the conduct of any investigation that may be carried out in connection with the use of the Card enrolled in the eWallet.

**5.9.4.7** The eWallet and associated mobile device may use certain security features and procedures to protect against unauthorised use of any Card. These features and procedures are the sole responsibility of the device provider. By enrolling the Card in the eWallet the User is obliged not to disable any of these security features of the associated Wallet/mobile device and to use them to protect all his/her Cards enrolled in the eWallet. The Bank does not control these security methods and is not responsible for how the eWallet provider and/or mobile device provider uses them.

**5.9.4.8** The Card User has the obligation to monitor the transactions carried out through the eWallet and to immediately notify the Bank by calling the Call Center Service of any discrepancy or irregularity identified in connection with them.

### **5.9.5 Limitations of liability**

**5.9.5.1** If the Bank is not the supplier of the eWallet, it does not offer any guarantee regarding its use; it is not responsible and shall not be liable in any way for any defect, delay or malfunction of the eWallet. The use of the Card within the eWallet may be affected by events beyond the Bank's control, and the Bank shall not be liable for any claims/claims for damages/indemnification arising out of or in connection with the use or inability to use the Card within the eWallet.

**5.9.5.2** The Bank shall not be liable for the legality of the provision/provision of the products/services of the device provider and/or third parties, nor for the security, accuracy, legality or any other aspect of the products/services provided by them.

**5.9.5.3** The Bank shall not be liable if the User's and/or the Card's data are used by the eWallet provider or by third parties with whom they collaborate for purposes other than those related to making payments through the eWallet, neither for the period during which the card is used in the eWallet, nor after its removal from the eWallet.

**5.9.5.4** It is the Card User's responsibility to read and understand the provisions of the agreements and/or terms of use made available by these third parties before creating, activating or enrolling/using the Card in an eWallet.

**5.9.5.5** The Bank is not responsible for and does not provide support or assistance for any third party hardware, software or other products or services. If the User has any questions or problems with a product or service offered by a third party, the User should contact that supplier/third party for assistance.

**5.9.5.6** The Bank is not responsible for the security of the mobile device on which the eWallet is installed nor for its operation, the Bank being liable to the Card User only for the fulfilment of its legal obligations as issuer of the Card.

**5.9.5.7** The Bank cannot control the operating system of the mobile device used by the Card User. The Bank is therefore not liable for any damage caused to the mobile device, including but not limited to any security breach caused by viruses, errors, deception, tampering, omission, interruption, malfunction, delay in operations or transmissions, computer lines or network failure or any other technical malfunction caused. The Bank cannot be held liable for direct or indirect damages resulting from the execution of unauthorised payments caused by the exposure of the Card User's device to viruses and/or other applications/programs, as well as theft.

## **5.10 Final provisions concerning the Card**

**5.10.1** The contract for the issuance and use of the Card shall be supplemented with the Card-specific provisions of the contractual documentation signed by the Client and the Bank, as well as with the provisions of the CGB.

**5.10.2** The contract for the issue and use of the Card is concluded for an indefinite period of time and comes into force at the time of the Card being handed over to the Primary Card User.

**5.10.3** The Bank may amend the provisions of the Agreement for the issue and use of the Card by notifying the Card User of the amendment to the contractual terms at least 2 months before the proposed date of its application, in accordance with the terms and conditions set out in sections 8.1 and 8.2 of the CGB.

**5.10.4** The contract for issuing and using the Card shall terminate in one of the following situations:

- a) by written agreement of the parties;
- b) by unilateral termination, at any time during the term of the contract, by the Card User or the Bank;
- c) in the event of the death or incapacity of the Primary Card User;
- d) by terminating the Debit Card Contract in accordance with clause **5.10.7** below;
- e) in case of force majeure or fortuitous event;
- f) by withdrawal of the product by the Bank;
- g) in the event of closure of the Current Account to which the Debit Card is attached;
- h) in any other cases provided by law;

**5.10.5** Unilateral termination of the Contract for the issue and use of the Card as per 5.10.4 b) may be requested:  
**(i)** by the Primary Card User by submitting a written request to any of the Bank's offices. The Bank will notify Card Users via the raiffeisen.ro website if other channels will be made available to them for submitting a request for unilateral termination of the Contract for the issue and use of the Card.

**(ii)** by the Bank by written notice to the Primary Card User, sent 2 months prior to the proposed date of termination of the Agreement. The notice shall be given in accordance with the provisions of section 8.2.

**5.10.6** At the latest on the working day following the registration of the Card User's request to terminate the Card Issuing Agreement, the Bank will block access to the Current Account via the Card if there are no transactions pending settlement.

Otherwise, access to the account will be blocked after all transactions made with the card have been settled.

**5.10.7 (1)** The Bank shall be entitled to terminate the Debit Card Agreement by operation of law, without notice and without the intervention of the courts, in any of the following cases:

- a) Failure by the Card User to comply with the contractual clauses, the conditions of Card operation imposed by the Bank, the legal provisions in force (such as, but not limited to, legal provisions on the prevention and combating of money laundering and terrorist financing and compliance with International and US Sanctions) or the Bank's working rules;
- b) Registration of Card transactions as suspicious or fraudulent;
- c) The Bank has identified suspicions of fraud/money laundering/terrorist financing/violation of International/US Sanctions;
- d) The seizure measure has been applied to the Card User's assets;

- e) The Card User is suspected of carrying out operations that violate legal or contractual provisions;
- f) For the Card User's Accounts, requests for return of funds have been received from the ordering/correspondent banks on suspicion of fraud, money laundering, terrorist financing, violation of International/US Sanctions, or
- g) The Bank has received information from banks or authorities in Romania or abroad regarding the Client's suspicion of fraud / money laundering / terrorist financing / violation of International/US Sanctions,
- h) the Card User becomes a Designated Person or Restricted Party or becomes subject to International Sanctions or embargoes imposed by the European Union, the Swiss Confederation, the United Kingdom of Great Britain and Northern Ireland, the United States of America, other States or any of their agencies, regardless of whether the Card User is directly or indirectly affected by such International Sanctions or embargoes,
- i) if the Card User has provided the Bank with false information and/or documents or refuses to provide the Bank with the requested information and/or documents, including on the basis of Articles 3.1.4 and 4.3.7 and/or agreements necessary for the Bank to fulfil its contractual and/or legal obligations (including for the purposes of FATCA and/or CRS requirements);

(2) In the cases referred to in the previous paragraph, the Bank shall notify the Customer of the measure taken, within 3 working days of the decision, in accordance with the rules in section 8.2 "Notifications".

(3) If there are transactions made with the Card pending settlement, the Bank may block the payment instrument from trading until all transactions are settled and the Card is terminated.

**5.10.8 (1)** If the User does not take possession of the Debit Card issued on a physical medium (plastic) within 6 months of its issue/reissue/renewal, it will be destroyed. If the debit card is used in a digital environment, it may continue to be used in a digital environment for transactions on the internet or through Electronic Wallet applications, even if the physical (plastic) card has been destroyed.

(2) To obtain another debit card issued on physical (plastic) media, the Customer may reissue it from Smart Mobile, call the Call Center service, or visit any Bank branch to request the issuance of a new debit card on physical media.

(3) If the Customer does not take possession of the physical debit card and does not use the card in the digital environment (card transactions registered in Electronic Wallet applications), within 6 months from the date of issue, reissue, or renewal, the debit card agreement shall terminate automatically at the end of this period, without any prior notice or other formality.

**5.10.9** The principal card user or his/her legal representative/successors are obliged to cover any amounts due in full upon termination of the contract. Any debit not covered by the Principal Cardholder arising from the use of the Card must be repaid by the Principal Cardholder to the Bank. In the event of termination, the Client shall be obliged to pay the fees and commissions relating to the Transactions carried out up to the date of termination.

**5.10.10** Termination of the Agreement at the Bank's initiative shall in no way affect the Bank's right to recover any amounts owed by the Primary Card User as a result of actions taken or not taken by the Primary Card User prior to the date of termination.

## **6. SPECIAL SERVICES OFFERED BY THE BANK THROUGH RAIFFEISEN BANK'S CALL CENTER SERVICE**

**6.1** The Bank's Call Center service allows access to the special services mentioned in this section through the telephone with the help of the telebanker or through the interactive automatic support application (virtual operator). The Call Center service is available in Romanian and English, except for services accessed through interaction with the virtual operator, which are available only in Romanian.

**6.2** Access to the Call Center telephone service through the interactive automatic support application (virtual operator) is not available to customers who do not have Romanian citizenship and call the Call Center service from a telephone number other than the one declared in the relationship with the bank, as well as to Visa Signature, Visa Infinite, World and World Elite credit card users, regardless of citizenship/residence.

**6.3 (1)** The user will prove its identity each time it uses the Call Center service, with the help of the Security Password in relation to the Bank.

(2) Customers holding the Raiffeisen Direct TOP service are identified by applying strict Client authentication under the conditions provided in the specific Contract.

**6.4** The special services that can be accessed through the telebanker are the following:

- a) Report the loss/theft of the Card or other emergency situations;
- b) Block access to the Account through the Card reported as lost/stolen and re-issuing the Card and the corresponding PIN code;
- c) Unlock the access to the credit card account through the credit card, if the lock was established at the Bank's initiative, as well as the unlocking the access to the Account through the debit card, provided that the blocking of the access was requested on the same day through the Service Call Center, as well as the Card User being in possession of the Card in the interval between the two requests, according to his statement; if these conditions are not met and the User requests the unlock, the Bank will proceed to replace the Card;
- d) Query of the balance of the Account to which the debit card is attached, respectively of the available funds in the Credit Card Limit, of the history of transactions related to the card, as well as of the Card status; the additional user can request information exclusively on the transactions made with the additional card of which he is the holder;
- e) Temporary modification of the daily limit of:
  - ATM/MFM cash withdrawal via Card, for the period indicated by the Primary User (for both Debit Card and Credit Card). Temporary modification of the limit can be requested only once per quarter (only once within each of the following intervals: 1 January - 31 March, 1 April - 30 June, 1 July - 30 September, 1 October - 31 December). The cash withdrawal limit for each type of Card, as well as more information on temporary changes to the limit at the Customer's request, its validity period, etc., can be found on the website [www.raiffeisen.ro](http://www.raiffeisen.ro) - section "In your support";
  - Card transactions at points of sale ("EPOS") and e-commerce.
- f) Provide information to the main Card user about the status of the request for the discovery of the account/credit limit, as the case may be, the parameters of the limit of account discovery/credit limit granted by the Bank in the Current/card account to which the Card is attached;
- g) Change credit card information: activating the Credit Card; add/modify/waive the direct debit service; modify the date of issue of the Activity Report; modify the Bank's agency where the Card will be transmitted; changing the Card password; correct personal data or contact details; the request of a document containing information of the Activity Report; register the refusal to increase the credit limit; initial setting and modification of the parameters related to the payment facilities in instalments of the amounts used from the credit limit, according to the specific Contract;
- h) Block the additional credit card or changing the access limit of the additional card;
- i) Waive optional insurance services attached to the Credit Card.
- j) Obtain the Bank's support regarding the registration/blocking/deletion of the Cards in the Electronic Wallet.
- k) Obtain Bank support on accessing and using Smart Mobile service.

The service provided for in point e) is available through the telebanker for customers who do not have the Smart Mobile application or for requests exceeding the transaction limits through the Card offered by the Smart Mobile application.

**6.5** The special services that can be accessed through the virtual operator are the following:

- a) Block access to the Account through the Card reported as lost/stolen and re-issue the Card and the corresponding PIN code; this service is available for the primary and additional Debit Card User ;
- b) The balance of the account to which the debit Card is attached respectively the available credit card limit, exclusively for the Main Credit Card User;
- c) Obtaining a ministatement (service available only for the main Debit/Credit Card Users), containing information regarding the debtor or creditor operations (depending on the request made expressly by the Main Card User in the virtual operator module) performed in connection with the Account to which is attached the debit/credit card, respectively the last five debits, the last five creditors or the last five transactions settled for the main Debit Card User and the last five transactions, debtor or creditor, made after the latest Activity Report for the User has been issued principal of credit card (in the case of Card transactions related to the Credit Card, only the settled transactions will be mentioned);
- d) Activate the Credit Card for the Main User;
- e) Obtain information about the latest Activity Report issued for the Credit Card: due date, minimum payment amount, total debt, exclusively for the Main User;

f) Request the unlocking of access to the Raiffeisen Smart Mobile Service for the main Card users who hold such services, as long as such functionality of the respective service is available.

## 7. TERMS AND CONDITIONS FOR THE DIRECT DEBIT SERVICE

### Define the used terms

Payment beneficiary = expected recipient of the funds of a direct debit payment operation; the legal person, supplier of goods and / or services, who has concluded with the institution to which the account has opened a commitment regarding the direct debit and who holds claims on the payer or the person in whose name the payment is made (the third party subscriber);

Payer = holder of a payment account that agrees with making a direct debit payment; he concluded a direct debit mandate with the payer's institution;

the person on whose behalf the payment is made (third party subscriber) – beneficiary's client, for whom the payer accepts to make payments to the beneficiary from its payments account;

Beneficiary's institution = the institution to which the beneficiary has opened the account to be credited or has been credited with the amount provided in the direct debit instruction; the institution that receives a direct debit instruction from the beneficiary, for the purpose of executing this instruction;

Payer's institution = the institution to which the payer has opened the payment account to be debited with the amount provided in the direct debit instruction;

the payer's institution and the beneficiary's institution may be one and the same bank if the payer and the beneficiary have an account opened at the same bank;

Direct debit commitment = the agreement concluded between the beneficiary and the beneficiary institution, which includes the beneficiary's responsibilities, as well as the beneficiary institution's acceptance regarding the beneficiary's use of the direct debit instructions;

Direct debit mandate (hereinafter referred to as "Mandate") = agreement of will, signed or whose authenticity has been verified by applying a security procedure by which the payer gives an authorization to a beneficiary to issue direct debit instructions on the account or the paying institution to debit his account with the amount and due provided in the direct debit instructions issued by the beneficiary; Each mandate will be highlighted in the payer's and beneficiary's bank system with a distinct identifier, mentioned on the mandate. The mandate may be given for a determined or indefinite period, with the possibility of subsequent revocation it can also cover a single payment or multiple payments of fixed or variable values;

Direct debit instruction = payment instruction initiated by a beneficiary on the account of a payer opened at the payer's institution, according to a mandate regarding direct debit; the payment operations are executed by the automatic debit of the payer account and the crediting of the beneficiary's account with the value of the debts that the beneficiary holds over the payer or the Person in whose name the payment is made (to the third party subscriber);

Payment date = the due date communicated to the payer/the person on whose behalf the payment is made (to the third party subscriber) and to the payer's institution by the beneficiary, or, as the case may be, the working day following the due date, if the due date is a non-working day, the date on which it is made debiting the payer's account with the payment transaction initiated by the Beneficiary and the related commission; At this date the Payer must provide in the account the amount of money necessary to make the payment and to pay the related commission;

Maximum limit = the maximum amount of the value of an invoice which the Payer can reasonably expect, taking into account the profile of the previous expenses and the conditions in the contract concluded with the Beneficiary. It is mentioned in the direct debit mandate given by the payer.

Account – the payment account indicated by the Payer in the direct debit mandate from which the payments to the Beneficiary will be made;

the person receiving (the final beneficiary) - entity in favour of which the payment will be made, through the beneficiary.

Date of first collection - the date from which the beneficiary is entitled to initiate direct debit instructions of the Payer's account;

Date of last collection - the date by which the beneficiary is entitled to initiate direct debit instructions of the Payer's account.

Singular payment – transfer of funds made from the Payer's account to the beneficiary's account, based on the direct debit mandate, which is executed only once;

Recurrent payment - transfer of funds from the Payer's account to the beneficiary's account, based on the direct debit mandate, which is executed repeatedly, during the term of validity of the mandate.

Within the Direct Debit Service regulated in the present section the Bank has the quality of the Paying Institution. The Direct Debit Service is offered to all the clients of the Bank, based on the provisions of the present section, which becomes active when issuing at least one Direct Debit Mandate.

### 7.1 Issue the Direct Debit Mandate

If the Client chooses to use the Direct Debit Service, he must issue at least one Direct Debit Mandate in one of the following variants:

- a) by signing the specific form in the Bank's agencies;
- b) by signing the specific form at the Beneficiary's premises - exclusively in the event that the Beneficiary offers this option;
- c) by accessing this option within the Smart Mobile Service;
- d) by requesting the activation of this mandate within the Raiffeisen Direct TOP Service.

Within the Direct Debit Service the Paying Client can issue an unlimited number of Direct Debit Mandates.

### 7.2. Activate the Direct Debit Mandate

**7.2.1** In the hypotheses provided for in point 7.1. letters a), c) and d), the direct debit mandate is activated within one working day. The Payer's Institution undertakes to inform the Beneficiary about the mandate concluded by the Payer, directly or through the Beneficiary's Institution.

**7.2.2** In the hypothesis provided in point 7.1. letter b), the beneficiary will send the mandate of the Paying Institution, for verification. If, after the verification, the Payer's Institution finds that it does not comply with the minimum conditions of validity (it does not have all the mandatory fields completed, the payer's IBAN account is not correct, inconsistency between the data entered on the mandate and those in the bank's records, declared previously paid, the signature specimen does not correspond), it will reject the mandate. If the mandate is rejected, the Payer's Institution will inform the Beneficiary about the non-activation of the mandate. A Mandate is considered active and produces effects from the moment it is confirmed by the Payer's Institution. The payer's institution commits to validate the mandate concluded by the Payer at the Beneficiary's headquarters or to refuse the activation within a maximum of 5 working days from the date of its receipt from the Beneficiary/Beneficiary's Institution.

**7.2.3** In order to activate the mandate issued according to 7.1. lit. b), in case the Bank decides to carry out the requests for clarification / completion of the mandate by telephone, the Payer expresses his agreement that, if all the fields in the mandate form are not completed or there is a mismatch between the completed and existing information in the Bank's database, be contacted by telephone by an employee of the Bank at the telephone number indicated to the Bank in the specific forms, in order to clarify the information. In order to identify the payer, the Security Password will be requested in relation to the Bank. The identity of the Payer will be considered proven after he has provided, at the request of the Bank's employee, the identification elements mentioned above. The payer assumes responsibility for the correctness of the information provided during the telephone conversation with the Bank employee. Expressly and in all cases, the Payer accepts that for the security of the information communicated the Bank has the right to record all telephone calls between the Payer and the Bank and acknowledges the probative force of recording the calls requested by the Bank and communicates the information regarding the Mandate; it also accepts that the steps mentioned in this article, in order to activate the Mandate, represent an option of the Bank, not an obligation of the Bank.

### 7.3 Execute the Direct Debit Mandate

**7.3.1** By issuing the Direct Debit Mandate, the Payer expresses his consent and mandates the Payer's Institution that based on his written instructions, included in the mandate, to make by debiting the Account the automatic payment of the amounts requested by the Beneficiary, corresponding to the invoices issued periodically by him on behalf of the Payer or of the person on whose behalf the payment is made (to the Third party subscriber).

**7.3.2** The Bank will not operate the payment of any invoice that exceeds the Maximum Limit completed by the Payer in the mandate.

**7.3.3** In order to execute the mandate, the Payer undertakes to provide in the Account, on the Payment Date, the amount necessary to make the payment and to cover the commission arising from the provision of this service.

**7.3.4** Also, the payment will be made only when the Payer's Account is not blocked as a result of an unavailability measure taken by the Bank or disposed of by an organ having such competences/attribution. No partial payments will be carried out.

**7.3.5** If, on the Payment Date, the payment in the Payer's Account does not fully cover the amount of the invoices, including the commissions related to the service provision, the Bank reserves the right not to make the payment. If the Bank decides, in accordance with its internal rules, to make a payment requested by the Beneficiary that exceeds the limit available in the Account, the provisions of section 3.4 of this document (discovered by unauthorized account / unauthorized overdraft) will apply. If the Payer does not wish to benefit from this facility, he must indicate to the Bank, in writing, in any banking or telephone unit, through the Call Center Service (assuming he also holds the Card User status), his refusal to make payments based on any Mandate above the limit available in the Account.

**7.3.6** Payment applications will be processed by the paying institution in the order of the dates indicated by the Beneficiary, until the use of the account available.

**7.3.7** The mandate granted by the Payer will be executed by the Bank starting with the first invoice to be delivered by the Beneficiary to the payment after the date on which the Payer requests to start the service.

### 7.4 Costs applicable to the Direct Debit Service

For each payment made on the Payer's Account at the request of the Beneficiary, the Bank will charge the Payer a commission whose value is set out in the list of fees and commissions applicable to the current account. The payer authorizes the Bank to automatically withhold this commission from his account, once the invoice is paid. The Bank may exempt the Payer from the payment of the commission or may charge a reduced level of the commission if the Cost reductions for the Payers have been agreed with the Beneficiaries, during the validity period of the conventions stipulating these reductions, concluded between the Beneficiaries and the Bank or if they have cost reductions were agreed between the Bank and the Payer, based on other contracts concluded between them, during the validity period of these contracts.

### 7.5 Change of the Mandate

**7.5.1** The payer can unilaterally modify the direct debit mandate, regarding the account from which the payments are made, the fixed/maximum limit, the identifiers for the invoice holder, by completing and submitting the modification form mandated to any unit of the Bank or the Beneficiary (only in if the beneficiary offers this option), or by requesting the modification through the Raiffeisen Direct TOP service or the Raiffeisen Smart Mobile service, if the Payer has any of these services. If the Payer wishes to indicate another payment account, the new account must be opened at Raiffeisen Bank.

**7.5.2** The changes made to the Direct Debit Mandates, communicated directly to the Payer's Institution (if the change was requested in the Bank's agencies, through the Raiffeisen Direct TOP service or Raiffeisen Smart Mobile), are opposable to it within one business day. In case the modification is requested at the Beneficiary's premises, the Beneficiary will submit the modification form to the Payer's Institution, for verification. If, after the verification, the Payer's Institution finds that it does not respect the minimum conditions of validity (it does not have all the mandatory fields completed, the payer's IBAN account is not correct, inconsistency between the data recorded on the request and those in the bank's records, declared previously by the payer, the signature specimen does not correspond), it will not operate the mandate modification. In case of rejection of the modification form, the Paying Institution will inform the Beneficiary about this. The payer's institution commits to validate the modification form submitted by the Payer at the Beneficiary's headquarters or to refuse its

implementation within a maximum of 5 working days from the date of its receipt from the Beneficiary/Beneficiary's Institution, until then the Payer's Institution using only the initial instructions.

The Payer's Institution will not be held liable for any damages suffered by the Payer/Third party subscriber and/or Beneficiary, due to the non-announcement of the modification of the initial payment instructions given by the Payer to the Bank.

**7.5.3** The granted mandate(s) remain valid if for technical reasons the Beneficiary makes a modification of the subscriber code initially assigned, notifying this change to the Bank and the Payer/third party subscriber.

## **7.6 Refusal to pay and right to refund**

**7.6.1** The payer may request the Paying Institution to refuse the following direct debit instruction received from the Beneficiary, by filling in a refusal form, in any bank agency, through the Raiffeisen Direct TOP Service or Raiffeisen Raiffeisen Smart Mobile. The application must be submitted no later than one business day before the due date of the debit instruction.

**7.6.2** The payer has the right to request, in maximum 8 weeks from the debit of the account or by the Bank under the Mandates, by submitting a written request to any unit of the Bank, to refund the amount paid to the Beneficiary's order, including the commission charged for the operation, if the value the payment transaction exceeds the amount that would have been reasonably expected taking into account the profile of its previous expenses and the circumstances relevant to the respective case (Maximum limit indicated in the mandate).

**7.6.3** The payer has the right to request, within a maximum of 13 months from the debit of the Account or by the Bank, by submitting a written request to any unit of the Bank, the refund of the amount paid, including the related commission, if there was no mandate in this respect.

**7.6.4** The payer will not be entitled to any refund if:

- a) the payer expressed his consent to execute the payment operation directly to the Bank;
- b) if applicable, information regarding future payment transactions was transmitted or made available to the payer, in the agreed form, at least 4 (four) weeks before the due date, by the Bank or the Payee Beneficiary.

## **7.7 Duration and termination of the Direct Debit Mandate**

**7.7.1** The direct debit mandate ends for an indefinite or determined period. The mandate ceases in one of the following situations, the Payer being obliged to pay the commissions related to the operations performed until the date of termination:

- a) by agreement of the parties, expressed in writing;
- b) by unilateral denunciation by one of the parties;
- c) in the case of the death of the Payer;
- d) by termination, in case one of the parties does not fulfil its contractual obligations or performs them improperly. Termination operates in full, without summons, delay and without the intervention of the courts. The party having the measure of termination shall notify the other party of the measure disposed of on the same day that the measure was taken;
- e) in case of force majeure according to article 7.10;
- f) by withdrawing the product by the Bank, with a minimum notice of two months;
- g) at the end of the validity period indicated in the Mandate;
- h) if for 36 consecutive months no payment was made through the Direct Debit Service due to the fact that the Beneficiary did not send to the Bank during this period any payment instructions or that at the date of payment the existing available in the payer account did not allowed the Bank to execute the payment instruction transmitted by the Beneficiary;
- i) in any other cases provided by law;
- j) in case of termination for any reason of the contract related to the Mandate concluded between the Payer / the person in whose name the payment (third party subscriber) and the Beneficiary are arranged;
- k) in case the Payer requests the closing of the Mandate Account or if it is closed or blocked for other reasons, without the Payer indicating to the Bank another account from which payments will be made to the Beneficiary.

**7.7.2** The payer must notify the Bank in writing, to any of its units or through the Raiffeisen Direct TOP service, if he is a client and of this service, in connection with the termination of the legal relationship between it or the

person on whose behalf the payment is made (the third party subscriber) and Beneficiary. The Bank will not be held liable for any kind of damages suffered by the Payer and / or Beneficiary, due to not announcing this fact.

### **7.8 Unilateral termination of the Mandate**

**7.8.1.** The payer may request the Bank to cease the payment service, for any of the Mandates given to the Bank (for him or the Subscriber Third Party, as the case may be) by a written request, filed and registered in any unit of the Bank or the Beneficiary, through the Raiffeisen Direct TOP service, if you are a customer of this service or through the Raiffeisen Smart Mobile service. The denunciation requests filed at the Beneficiary's headquarters becomes opposable to the Payer's Institution within 5 working days from the receipt of the denunciation form from the Beneficiary/Beneficiary's Institution, until the expiration of this term the Bank will consider the Mandates as active and will execute them, in the case to such a request from the Beneficiary,

**7.8.2** The payer has the obligation to pay the fees and commissions related to the operations performed until the date of termination.

**7.8.3** The Bank may unilaterally terminate the direct debit mandate with a minimum notice of two months.

### **7.9 Provisions regarding the relationship between the Beneficiary and the Payer**

**7.9.1.** The payer authorizes the Bank to notify the Beneficiary / Institution of the beneficiary about the Mandate he has granted, as well as of any request for modification or termination of the mandate and to communicate to the Beneficiary any necessary information regarding the execution of the Mandate and to transmit to them, directly/via Transfond (as the case may be), personal information that may be contained in the Mandate. The payer declares that it is authorized by the third party subscriber to transmit his personal data for the purpose of processing.

**7.9.2.** The Bank shall not be held liable for any damages caused by the Payee Beneficiary or the person on whose behalf the payment is made (Third party subscriber). Any misunderstandings regarding the amount entered by the payment beneficiary (the Beneficiary) in the payment instructions communicated to the Bank and executed by the Bank under the Mandates, the amount of the invoices, the non-communication or defective communication by the Beneficiary to the Bank of the amount and/or the maturity of the invoices, at the agreement between the amounts stipulated in the invoices and the amounts requested to be paid by the Beneficiary, to the amounts debited or to the amounts refused to pay due to the lack of availability or at the express request of the Payer, will be solved according to the provisions of the contract concluded between Payer / Third party subscribed with the Beneficiary.

### **7.10 Force majeure**

The force majeure exonerates of liability the party that invokes it, according to the law, after the notification of the other party. The party invoking the force majeure will notify the other party within a maximum period of 5 days from the occurrence and will transmit the supporting documents, certified by the Chamber of Commerce and Industry of Romania according to the law, within 15 days. In the same conditions, the case of force majeure will be communicated.

### **7.11 Final provisions**

**7.11.1** If the direct debit mandate is issued through the Raiffeisen Smart Mobile service, the provisions of the Raiffeisen Smart Mobile contract will be applied with priority.

**7.11.2** Changes to the terms and conditions of the Direct Debit Service are made on the basis of the express or tacit agreement of the parties. The Bank has the obligation to notify the Payer of the modification of the contractual clauses at least two months before the proposed date for its application. The payer has the obligation to communicate in writing the option of accepting or not accepting the new conditions within the two-month period mentioned above. If by the proposed date for payment the Payer does not notify the bank, in writing, at any of the Bank's territorial units, the failure to accept the changes, the Parties agree that the payment of the Payer is tacit acceptance of the respective changes. If the Payer notifies the bank that it does not accept the changes proposed by the Bank, before the proposed date for applying the changes, the Payer has the right to unilaterally terminate the contract, immediately and free of charge, under the conditions provided in art. 7.8.

**7.11.3** Any request of the Payer to the Bank, in connection with the activation, execution, modification or termination of the Direct Debit Mandate, submitted in writing, must comply with the standard forms provided by the Bank and/or Beneficiary, otherwise it will not be binding to the Bank.

**7.11.4.** Any dispute arising between the Bank and the Payer in connection with the conclusion and execution of this Agreement will be settled amicably or, if this is not possible, by the competent courts, according to the Romanian legislation in force. In order to amicably resolve any disputes (including disputes regarding the right to reimbursement provided for in Art. 7.6. The payer may notify, according to the law, the National Consumer Protection Authority and/or the National Bank of Romania, in order to apply the extra-judicial procedures to resolve the dispute.

## **8. FINAL PROVISIONS**

### **8.1. Conclusion and modification of specific Agreements and the GBC**

**8.1.1** For the conclusion of a specific Contract, as well as for any other requests/applications/declarations/forms used in interaction with the Bank, the Customer's Consent may be expressed, as appropriate::

- a) by the hand/electronic signature, under the conditions agreed by the parties;
- b) by telephone during the recorded calls, made through the Call Center Service or in another agreed mode that involves a telephone call, to the extent that the Bank offers the Client these means;
- c) within the remote access electronic applications offered by the Bank, such as, but not limited to mobile-banking application, by using the sets of rules for the identification and authorization specific to each application separately, provided for in the Specific Agreements/terms and conditions related to applications;;
- d) by any other method agreed by the Bank with the Client in the specific Agreement;
- e) through any behavior agreed upon by the Bank and which leaves no doubt as to the intention to produce the corresponding legal effects.

**8.1.2. (1)** The Consent for the conclusion of these GBC shall be only expressed by all Parties using the same signature method, respectively:

- (i) the handwritten signature of the document in the presence of a Bank representative;
  - (ii) affixing an electronic Signature on the document in electronic format, agreed by the Bank.
- (2)** Signing GBC in electronic format, with the electronic signature may be performed only by means of communication agreed by the Bank and shall be deemed as concluded at the Bank's headquarters.

**8.1.3.** The changes made to the Specific Contracts and the GBC are communicated to the Client according to the "Notifications" section or through the communication means specific to each service/product according to the specific Agreement.

**8.1.4.** The Bank and the Client agree that any modification proposed by the Bank regarding the clauses in the GBC and/or the Specific Contracts shall be notified to the Client at least two months before the proposed date for its application.

**8.1.5.** If, until the proposed date for applying the changes, the Client does not notify the Bank in writing of not accepting the changes, at any of the territorial units of the Bank or in the modalities provided for in the specific Contracts, the Bank and the Client agree that the silence of the Client values tacit acceptance of those modifications, if the legal provisions in force do not regulate the contrary.

**8.1.6.** The continuance of the contractual relations between the Bank and the Client is not possible in the absence of a Client's agreement, tacitly or expressly, regarding the contractual changes notified by the Bank.

**8.1.7.** The Bank will automatically apply the specific legal provisions of imperative character regarding the services /products offered to the Client, including for the credit products, insofar as they differ from those established in the specific Contracts, without having to modify these GBC.

### **8.2. Notifications**

**8.2.1.** Any requests, notifications, approvals, communications ("the Notification") arising from these GBC and/or the specific Agreements concluded between the Bank and the Client will be made by the Bank in writing, the Notification can be submitted personally and/or transmitted by post and/or or by fax and/or e-mail and/or SMS text message, at the address (postal and/or e-mail), respectively at the contact numbers (fax or mobile

phone), as indicated by the Client through the communication channels made available by the Bank to the Client for this purpose or by a message posted within the Smart Mobile application, in-app banner notifications in Smart Mobile, push notifications in Smart Mobile for the holders of these services or by posting on the Bank's website with personalized access.

**8.2.2.** The notification or any other communication is considered received by the Client, **(i)** in the case of personal remittance upon delivery, **(ii)** in the case of transmission by fax/e-mail/SMS - on the date of generation by the apparatus used for transmission, of the transmission report **(iii)** in the case of postal dispatch - within 3 working days for the dispatches on the Romanian territory, respectively within the term guaranteed by the postal and courier service providers for shipments abroad and **(iv)** in case of transmission of the message within the application Smart Mobile, for the holders of these services - - at the date of posting the message in the application Smart Mobile; **(v)** in case of push notifications/in-app banner notifications in Smart Mobile - on the date the message is posted on the mobile device screen.

**8.2.3.** Any written notification is considered validly sent by the Bank through the mail circuit, as the case may be by fax/e-mail/SMS, if it has been sent to the last postal and/or e-mail address, respectively to the last fax numbers or mobile phone communicated to the Bank by the Client.

**8.2.4. (1)** The Bank uses a single postal address in its relationship with its Customers for sending any correspondence (the Customer's home address or the correspondence address indicated by the Customer) in connection with all products/services contracted by them. The Bank shall send correspondence to **(i)** the home address (as communicated by the Customer at the time of the last data update) or **(ii)** if the Customer indicates a mailing address in relation to the Bank, to the last mailing address indicated by the Customer.

**(2)** The Bank reserves the right:

**i.** in relation to the home postal address – to verify whether there is current information regarding the Customer's home address in any credible and independent sources available, and to collect this information, to the extent that the Bank implements a data flow in this regard;

**ii.** in relation to the mailing address – to process any change of mailing address by the Customer within a maximum of 30 calendar days.

**8.2.5.** Any notification or other communication received by the Bank on a day after 16.00 of a working day, will be considered received on the following working day. Exceptions from this are the operations and documents regarding the payment services to which the deadlines are applicable;

**8.2.6 (1)** The client and the Bank agree that the answers to the complaints/appeals regarding the payment services will be sent by the Bank through one of the communication modalities provided in art. 8.2.1 above, in accordance with the terms and conditions provided by the payment services legislation.

**(2)** The replies to the complaints/appeals, other than those regarding the payment services, will be sent to the Customers within the terms and conditions provided by the special laws or within a reasonable term if the law does not impose a certain response time.

### **8.3. Applicable law. Disputes. Language of the contract.**

**8.3.1.** The relations between the Bank and the Client are governed by the Romanian legislation. Any disputes will be settled amicably. When this is not possible, the Client may call on extrajudicial mechanisms for the alternative settlement of disputes with the Bank or can be addressed to the courts, according to the procedural rules in force.

**8.3.2.** In order to amicably resolve any disputes regarding the lending activity, payment services and/or the processing of personal data, the Client may appeal to extrajudicial settlement procedures by notifying, according to the law, the National Authority for Consumer Protection, as the case may be (office at Bdul Aviatorilor no. 72, district 1, Bucharest, Tax code 24268010, Public Relations tel. 0759045333, e-mail [office@anpc.ro](mailto:office@anpc.ro)), the National Bank of Romania (office at Str. Lipsicani no. 25, district 3, Bucharest, code 030031, Tax code 361684, tel. 021.313.04.10/021.315.27.50) or the National Supervisory Authority for Personal Data Processing (office at B-dul G-ral. Gheorghe Magheru no. 28-30, district 1, Bucharest, tel. 318.059.211 , e-mail: [anspdcp@dataprotection.ro](mailto:anspdcp@dataprotection.ro)). If the Client decides to resort to alternative dispute resolution with the Bank, he may submit a request in this regard to the Alternative Dispute Resolution Center in the Banking field (CSALB), office at in municipiul Bucharest, Str. Sevastopol 24, 2nd floor, district 1, postal code 10992, Romania,

telephone 021 9414, website address [www.csalb.ro](http://www.csalb.ro) or he may apply to the mediation procedures reglemented by the legislation on mediation and organisation of the profession of mediator.

In order to amicably resolve any disputes regarding investment services and products, the Client may, in accordance with the law, refer the matter to the "Financial Supervisory Authority (supervisory authority with headquarters in Splaiul Independenței no. 15, sector 5, 050092, Bucharest, tel: 0800.825.627, 021.305.3470) or the National Bank of Romania at the contact details mentioned above.

**8.3.3.** These GBC are concluded in Romanian and English; any notifications or communications arising from this contract will be made in Romanian.

#### **8.4. Guarantee of bank deposits**

**8.4.1** The Bank is a participant in the Romanian Bank Deposit Guarantee Fund ("RDBGF"), therefore the Client's money held in bank accounts opened with the Bank is guaranteed within the limits set by the RDBGF and under the conditions established by the legal regulations in force in the field of deposit guarantee.

**8.4.2** The level of compensation paid by the Deposit Guarantee Fund shall be determined by deducting from the sum of all eligible deposits held by the Customer who is a guaranteed depositor with the Bank on the date on which the deposits became unavailable, the total amount of the Bank's outstanding claims against that Customer on that date.

**8.4.3** The Bank shall provide information on the guarantee of deposits by the RDBGF and the list of non-guaranteed deposits by posting it on its website at all its offices and by providing the Depositors' Information Form in paper and electronic format ([www.raiffeisen.ro/doc/fgdb-ro.pdf](http://www.raiffeisen.ro/doc/fgdb-ro.pdf)).

#### **8.5. Restrictions and interdictions**

**8.5.1.** If a law prohibits the Client from fulfilling any of its obligations towards the Bank (or any part of the respective obligation) in the currency in which it is established, or prevents any funds in that currency from being remitted to the Bank, the Client will fulfil its obligation or the respective part of it, making the payment to the Bank (at the Bank's choice and in the manner indicated by the Bank) in that other currency that the Bank will indicate.

**8.5.2.** The Client will pay a sufficient amount in that other currency so as to enable the Bank to purchase an amount equal to the payment obligation of the Client or the respective part thereof, in the currency in which it is established, calculated at the relevant spot rate as determined by the Bank. For this purpose, the Bank shall have the right to debit any of the Client's accounts, at its discretion, with the amounts owed by it, without prior notice to the Client, and the Client expressly authorizes the Bank, by the present, to sign the payment orders, the instructions and other documents that may be necessary for the above mentioned operation to be performed in full and accordingly.

#### **8.6. Cumulative and non-exclusive remedies**

Each of the rights/remedies/guarantees granted to the Bank on the basis of this document and/or the specific Contracts concluded between the Bank and the Client, may be exercised/executed by the Bank in the order chosen by the Bank, at its total discretion, regardless of the date of birth/constitution of these rights/remedies in his favour, and will be additional to all other rights and remedies granted to the Bank by virtue of any other agreement, any other guarantees or laws.

#### **8.7. Deductions or withholdings required by law**

If a deduction or withholding must be made, according to the law, from a payment of the Client to the Bank, the Client will pay a higher amount, so that after any such deduction or withholding, the Bank will receive and benefit from an equal net amount with the amount he would have received if no deduction or deduction had been made.

#### **8.8. Assignment. Novation. Transfer.**

The Bank may transfer in any way (assignment, novation, delegation or any other mechanism for transmitting the rights and obligations recognized by law), in whole or in part, any of its rights and obligations arising from the GBC/Specific Contract. The contract will be considered as concluded for the benefit and will give rise to a

valid and enforceable obligation for a buyer or a person who takes over the assets of the Bank, a successor of the Bank or any assignee or agent thereof. The client may not assign/novate/transfer/delegate to any third person, at any time, without the prior written consent of the Bank, his rights and obligations arising from this Contract.

### **8.9. Transmission risk**

If the Bank, at the Client's request, transmits sums of money, securities/trade effects/merchandise delivery documents to a certain recipient, using for this purpose third parties as intermediaries, the transmission is at the Client's risk. Any loss resulting from the Bank's use of postal, telephone, telex, fax, e-mail, SWIFT, courier or other means of communication or transport for this purpose will be borne by the Client with the Bank's exemption from any liability in this regard.

### **8.10. Force majeure and fortuitous event**

**8.10.1** Force majeure exonerates the party invoking it from liability, in accordance with the law, after informing the other party. The party invoking force majeure shall notify the other party within a maximum of 5 days from the occurrence of the force majeure and shall submit the supporting documents, certified by the Chamber of Commerce and Industry of Romania according to the law, within 15 days. Under the same conditions, the termination of the force majeure shall be notified.

**8.10.2** The Bank shall not be liable to the Client for losses caused by force majeure or fortuitous event (unforeseeable and unavoidable events beyond the control of the parties), including, but not limited to: Nationalization, expropriation, currency restrictions, measures by bodies with regulatory powers, including, but not limited to, any agency, governmental body, the National Bank of Romania, labor disputes among the Bank's personnel or other entities involved in transactions carried out by the Bank on behalf of the Client and whose services are used by the Bank, boycotts, power outages or power cuts in the Bank's communication network or equipment, international conflicts, violent or armed actions, acts of terrorism, insurrection, revolution, as well as unforeseeable natural events with major negative effects.

**8.10.3** In all cases in which the Bank's liability is incurred, it shall be limited to cover the direct and actual damage caused to the Client.

### **8.11. Other final clauses**

At any time of the contractual relationship, the Client has the right to receive, on request, on paper or on any other durable medium, a copy of these GBC.

## 9. CLIENT'S STATEMENTS AND THE PARTIES' SIGNATURES

9.1. The undersigned, Client, personally or, as the case may be, through or assisted by the Legal Representative, or by the Trustee, declare that: (tick, as appropriate, 9.1.a or 9.1.b):

9.1.a.  The bank offered me a copy of the GBC, in English and in a clear form, and that I was informed about the 15-day deadline I have at my disposal to decide if I accept the GBC on the above mentioned issues. As a result of the fact that I have read, understood and agree with the prior information made available by the Bank, I express my agreement regarding the reduction of the 15-day deadline and wish to sign the GBC today.

9.1.b.  The bank offered me, 15 days before the signing date of these GBC by the undersigned, a copy of this document:

on paper

by e-mail

9.2. This contract (General Conditions for the Conduct of Banking Operations, consisting of 9 Chapters 61 pages), having the following content: 1. Introduction; 2. General principles; 3. General conditions applicable to the accounts; 4. Provisions regarding the payment operations; 5. Contractual provisions relating to the issue and use of the Card; 6. Special services offered by the Bank through the Call Center of Raiffeisen Bank; 7. Terms and conditions for the Direct Debit Service 8. Final provisions; 9. The Client's Statements and the Parties' signatures, is signed by the parties in 2 copies, being concluded today, \_\_\_\_\_.

The client states that the Bank has communicated a copy of the GBC, according to its request:

on paper

by e-mail, at the address indicated by the Client and registered in the Bank's records

through the mobile banking service, as the case may be.

These GBCs replace the previous versions, except the section "Granting of credits" within them, which remains in force and continues to apply in relation to the clients who have taken loans during the period when these versions were in force.

**RAIFFEISEN BANK S.A.,**

**CLIENT:**

\_\_\_\_\_  
(surname, name)

\_\_\_\_\_  
(Client's surname, name, Personal code; must be filled in)

\_\_\_\_\_  
(signature)

\_\_\_\_\_  
(Client's signature)

\_\_\_\_\_  
(Proxy/legal representative's surname, name, Personal code, to be filled in when necessary)

\_\_\_\_\_  
(Proxy/legal representative's signature)

Date: \_\_\_\_\_

Date: \_\_\_\_\_