

**GENERAL BANKING CONDITIONS for INDIVIDUALS****01.10.2026****1. GENERAL PROVISIONS GOVERNING THE RELATIONSHIP WITH THE BANK****1.1. Introduction. Contents. Application rules****1.1.1. Introduction**

These General Banking Conditions establish the rules governing the relationship between the Bank and its individual clients.

They are supplemented with the forms specific to each product or service, applicable laws and regulations, the regulations issued by the National Bank of Romania, as well as customary banking practices and practices applicable at national and international level.

The Bank's identification details are:

- Name: BRD-Groupe Société Générale S.A.
- Address: B-dul Ion Mihalache nr.1-7, district 1, Bucharest, Romania
- Telephone: +4021.301.61.00
- E-mail: mybrdcontact@brd.ro
- Internet site (website): <http://www.brd.ro>
- Tax Identification Number 361579, VAT registration number: RO 361579
- Registration number with the Trade Register: J1991000608402
- European Unique Identifier (EUID): ROONRC.J1991000608402
- Registration Number in the Register of Credit Institutions: RB-PJR-40-007/18.02.1999
- CNVM Certificate No. 255/06.08.2008, registration number in the CNVM Public Register: PJR01INCR/400008.

**1.1.2. Contents.** The structure of this document is as follows:

1. General provisions governing the relationship with the Bank
2. Accounts and payment services – general rules
3. Special provisions applicable to types of products/services
  - 3.1. Current account
  - 3.2. Revolving account
  - 3.3. Savings products (3.3.1. Term deposits 3.3.2. Savings accounts. 3.3.3. Savings Service for Card Payments at POS Terminals
  - 3.4. Bank card
  - 3.5. Remote banking services ( 3.5.1. General Principles 3.5.2. MyBRD Contact service 3.5.3. MyBRD SMS Service)
  - 3.6. Account switching service
4. Product and service packages

**ANNEX.** Notification on the processing of personal data**1.1.3. Application rules**

**a) The contract.** These General Banking Conditions form the general framework in the Client-Bank relationship. Together with the annexes, contracts, applications and specific forms concluded by the Client for each product or service, as well as the Fee Guide, they constitute the Contract between the Client and the Bank.

**b) The general clauses** in chapter 1 (General provisions governing the relationship with the Bank) apply to all individual customers. They apply regardless of the type of product or service contracted.

**c) Specific clauses.** Each product or service also has specific clauses, which complement the general ones. They can be found in • other chapters or sections of this document, and in • the specific forms and contracts of each product or service.

**d)** In addition, for payment **products and services**, in addition to the general clauses (chapter 1) and the product/service-specific clauses (according to letter c) above), the provisions of chapter 2 (Accounts and payment services - general rules) also apply.

e) These General Banking Conditions replace the previous version of the General Banking Conditions. They also replace and supplement any contrary provision in specific contracts, forms or documents previously concluded by the client.

**1.2. Definitions**

For the purposes of these General Banking Conditions, the following terms shall have the meanings set out below:

- **3D Secure:** a security protocol for online card transactions on websites that support this service and display the logos: “Visa secure” or “MasterCard Identity Check”.
- **Acceptor:** means any: (i) entity (public institution or person, regardless of its legal form of organisation, duly authorised by law to carry out economic activities) that has entered into a card acceptance agreement with a financial institution; or (ii) unit of a financial institution or ATM that allows card transactions to be carried out.
- **ANAF:** National Agency for Fiscal Administration.
- **Apple Pay:** a digital wallet service provided by Apple Distribution International that enables the Client to add BRD-issued cards to compatible Apple devices using NFC technology – such as a mobile phone (smartphone), smartwatch, wristband, etc.
- **Authentication:** the procedure by which the Bank verifies the identity of the Client or the validity of the use of a payment instrument, including the Client’s personalised security credentials.
- **Strong Customer Authentication:** authentication based on the use of at least two of the following elements: knowledge, possession and inherence. These elements are independent of one another and protect the confidentiality of the authentication data.
- **Authorisation of a Payment Transaction:** the procedure by which the Payer expresses consent to the execution of a payment transaction. Depending on the payment instrument used, consent may be given in various ways:
  - a) by signature – when payment transactions are initiated on paper;
  - b) by using the personalised security credentials for remote banking services and cards, as set out in Sections 3.4 and 3.5. below.

In the absence of consent given in any of the forms specified above, the payment transaction shall be deemed unauthorised.

- **Bank or BRD:** BRD-Groupe Société Générale SA, including any of its local branches or offices (place of business, branch office, branch).
- **Beneficial Owner:** the natural person who ultimately owns or controls the Client and/or the natural person on whose behalf or in whose ultimate interest a transaction, operation or activity is carried out, directly or indirectly.
- **NBR:** National Bank of Romania.
- **Card:** electronic payment instrument. Through it, the Holder/User can access the funds in the account or accounts attached to the card.
- **Payment Incidents Register (CIP):** the structure within the National Bank of Romania (NBR) that manages information on payment incidents involving account holders in connection with cheques, bills of exchange and promissory notes.
- **Credit Risk Centre (CRC):** the structure within the NBR that manages information about credit risk and card fraud.
- **Click to Pay:** a secure remote payment functionality linked to the card, based on the international EMV Secure Remote Commerce (SRC) standard and implemented by Mastercard and Visa card

schemes. It enables cardholders/users to make online payments to merchants without having to manually enter their card details at the time of payment. For payment security purposes, the actual card details stored in Click to Pay are replaced with a secure token. Further details on this functionality are set out in Article 3.4.3.12 below.

- **Client:** any natural person who has negotiated a transaction relating to the Bank's banking activities with the Bank, even if the transaction has not been completed. A Client also includes any natural person who is or has been a beneficiary of the Bank's products or services, including an authorised signatory on an account.

- **A financially vulnerable client** is a client:

- a) whose monthly income does not exceed 60% of the average gross wage in the economy; or
- b) whose income in the last 6 months does not exceed the equivalent of 60% of the average gross wage in the economy.

The average gross monthly earnings in the economy taken into account are those forecast in the latest macroeconomic forecast (i.e. the autumn forecast) published by the National Commission for Strategy and Prognosis in the current year for the following year.

- **BIC code** (Bank Identifier Code): a unique code assigned to each bank and used to identify banks within the S.W.I.F.T. system. (Society for Worldwide Interbank Financial Telecommunication). The BIC code of BRD is BRDEROBU.
- **Unique Identification Code:** IBAN (International Bank Account Number) or other code that uniquely identifies a payment account.
- **MyBRD Contact:** the Bank's Customer Relations Service. You can call the following phone numbers:
  - 021 302 61 61 - standard-rate number that can be called from any network; or
  - \*BANCA (\*22622) - calls are charged at the in-network rate from any Orange, Vodafone, Telekom Mobile or RCS Digi Mobil number.

This service is available during the hours specified in the Contact section of the Bank's website.

- **Current account:** the underlying product for various banking products and services, used to execute payment transactions. Any reference to a current account shall also be deemed to include a reference to a payment account with basic features.
- **Online-accessible payment account:** a payment account that can be accessed by the payment service user through an online interface.
- **Payment account with basic services or current account with basic service:** a payment account that enables the following transactions to be carried out:
  - a) opening, managing and closing the payment account;
  - b) depositing funds into a payment account;
  - c) cash withdrawals from the payment account, within the European Union, at the counter or at ATMs, during or outside the credit institution's business hours;
  - d) within the European Union: direct debits; card payment transactions, including online payments; credit transfers, including standing orders, at bank terminals, at counters and through the credit institution's online banking facilities.

The payment account with basic services is available in Romanian lei. It is offered to Clients who do not hold another payment account with a credit institution in Romania (including a payment account with basic services), unless the Client declares that they have been notified of the closure of that account.

The fees applicable to this type of account may vary depending on the Client's status as a "financially vulnerable client" (as defined above).

- **Revolving account:** an account that gives the Client access to a credit line granted by the Bank through a credit card. This account records all transactions carried out using the credit card, as well as the related fees, interest and insurance premiums.
- **Contract:** these General Banking Conditions, together with their appendices, the agreements, applications and product- or service-specific forms entered into by the Client for each product or service, and the Fee Guide.
- **Exchange rate:** the rate used to calculate a currency exchange, provided by the Bank or derived from a public source.
- **Exchange rate applicable to card transactions:** the exchange rate applied to card transactions where the currency of the current account/revolving account differs from the transaction currency (or, where applicable, from the card scheme settlement currency). Additional details are available on the website [www.brd.ro](http://www.brd.ro).
- **Value date:** the reference date used by the Bank to calculate the interest applicable to funds debited from or credited to an account.
- **Direct debit:** a national or cross-border payment service enabling the payer's payment account to be debited at the initiative of the payee, based on the payer's consent.
- **Unauthorised overdraft:** the debit balance on a current account or any balance exceeding the credit limit granted for the current account or the revolving account. It results from payment transactions carried out through the account or from the Client's failure to pay amounts due (interest, fees, etc.). An unauthorised overdraft constitutes a payment obligation that becomes immediately due and payable from the moment it is recorded in the account.
- **Holder:** the individual who is the holder of an account and holds a card issued by the Bank.
- **Personalised security credentials:** confidential and personal credentials intended to be known only to the Client (they must not be disclosed to anyone under any circumstances, regardless of the context). They vary depending on the type of product or service, as follows:
  - (a) **For Cards:**
    - (a.1) **PIN code:** is the Personal Identification Number provided by the Bank and used for card transactions at bank terminals;
    - (a.2) **CVC2** (Card Verification Code) and **CVV2** (Card Verification Value) code: is a three-digit code printed on the back of the card, used for online transactions, mail, telephone or fax orders, or for enrolling the card in digital wallet services;
    - (a.3) The **e-Commerce Password** consists of a static password (defined by the Cardholder/User on the transaction authentication page) and a unique, dynamically generated code used to authenticate each online transaction on websites secured by 3D Secure (the "3D Secure Code"). The 3D Secure Code is sent by SMS to the Cardholder/User's mobile phone number registered with the Bank and remains valid for 15 minutes. This authentication method applies only to Cardholder/Users who do not use the BRD mobile banking application. The Bank may refuse transactions that are not authenticated using the e-Commerce Password;
    - (a.4) **Biometric authentication** uses biometric data through the Bank's mobile banking application to authenticate transactions made with cards enrolled in digital wallet services and online card transactions. Examples of biometric data include: Touch ID (fingerprint), Face ID (facial recognition);  
**Face ID** is a method that enables the device to recognise the Client by their face. It uses advanced technology that

enables the device to accurately recognise the Client's facial features;

(a.5) **Token PIN (mPIN):** a 6-character code defined by the Client upon first accessing the YOU BRD Service (the mobile banking channel), used to authenticate online card transactions;

(a.6) **Device PIN:** used to access digital wallet services.

**(b) For remote banking services:**

(b.1) for MyBRD Contact Service: MyBRD Contact ID and numeric access password;

(b.2) for MyBRD SMS Service: PIN

(b.3) for the YOU BRD internet and mobile banking service and other remote banking services: The personalised security credentials defined in the specific agreements entered into with the Bank.

➤ **Fee Guide:** The Fees and Charges Guide for Individuals, integral part of the Contract.

➤ **Google Pay:** a digital wallet service offered by Google. It enables the Client to register cards for use in transactions with NFC-enabled Android devices (e.g. smartphones, smartwatches, etc.).

➤ **BRD Group:** BRD, together with its subsidiaries and the companies affiliated with them.

➤ **Société Générale Group:** an international banking group conducting banking activities worldwide, of which the Bank is a member. Details about the structure of the BRD Group and the Société Générale Group can be found on the website: <https://www.brd.ro/despre-brd/noutati-si-presa/ultimele-noutati>.

➤ **IBAN (International Bank Account Number):** a combination of letters and numbers that uniquely identifies an account held with a payment service provider worldwide. The IBAN is assigned by the Bank to the Client when the account is opened. It appears on every account statement.

➤ **Debit instrument:** check, bill of exchange or promissory note.

➤ **Payment instrument:** a personalised device or a set of procedures agreed between the Client and the Bank that enables the transfer of funds from the payer to the payee. Payment instruments may be: (i) paper-based payment instruments; or (ii) electronic payment instruments (cards and remote electronic payment instruments).

➤ **Account Proxy:** the individual authorised to represent the Client, as the account holder, in dealings with the Bank. May be appointed when the account is opened or subsequently, by completing the Bank's forms or by means of an express notarised power of attorney.

➤ **Multicurrency:** an option that allows the Cardholder of a debit card denominated in Romanian lei to link to the card other current accounts in different currencies, held with the Bank in the Cardholder's name, in addition to the current account denominated in Romanian lei originally linked to the card. Details can be found in article 3.4.4.8 below.

➤ **Payment transaction:** an act initiated by the Client, as payer, or by the payee to deposit, transfer or withdraw funds into/from a payment account, irrespective of any underlying obligations between the Client, as payer, and the payee.

➤ **Payment order:** an instruction from the Client, as payer, or from the payee requesting the Bank to execute a payment transaction.

➤ **Standing order:** an instruction by which the payer requests the payment service provider with which the payer's payment account is held to execute credit transfers at regular intervals or on predetermined dates.

➤ **Card Organisation:** an international organisation (Visa, Mastercard, etc.) that establishes the terms and conditions of use of cards issued under its own brand.

➤ **Persons without legal capacity:** persons who, under the applicable law, do not have the legal capacity to enter into legal

acts on their own. They are represented by their legal representatives. In certain cases, the law also requires the approval or authorisation of other persons or authorities (e.g. the Family Council, the Guardianship Court). Persons without legal capacity include, for example, minors under the age of 14 and persons placed under special guardianship by a court or other competent authority.

➤ **Persons with limited legal capacity:** persons who, under the law, enter into legal acts with the consent of their legal representative. In certain cases, the consent or authorisation of other persons or authorities is also required (e.g. the Family Council, the Guardianship Court). Persons with limited legal capacity include, for example, minors who have reached the age of 14 and adults placed under judicial counselling by a court or other competent authority.

➤ **Cross-border payments:** foreign currency payment transactions (carried out abroad or within Romania) and Romanian leu payment transactions carried out abroad.

➤ **Domestic payments:** payment transactions in Romanian lei carried out within Romania.

➤ **Chargeback:** the procedure by which the Cardholder or Card User may dispute an unauthorised or incorrectly executed transaction.

➤ **Legal representative:** a person who enters into legal acts on behalf of a Client without legal capacity or gives consent to legal acts entered into by a Client with limited legal capacity. Examples of legal representatives include a parent, a guardian, a curator and a special curator.

➤ **Resident:** a natural person – whether a Romanian citizen, foreign national or stateless person – who is domiciled in Romania and holds identity documents issued in accordance with the law.

➤ **Remote banking services:** services that may be accessed remotely by the Client, such as MyBRD SMS, MyBRD Contact, YOU BRD and any other services governed by specific agreements.

➤ **YOU BRD service:** YOU BRD internet and mobile banking service. The terms and conditions applicable to this service are set out in a specific agreement entered into between the Client and the Bank.

➤ **Durable medium:** any instrument which enables a payment service user to store information addressed personally to that user in a way accessible for future reference for a period of time adequate for the purposes of the information and which allows the unchanged reproduction of the information stored.

➤ **NFC (Near Field Communication) technology:** technology that enables data to be exchanged between devices over short distances. It uses a high-frequency radio communication standard.

➤ **Terminals:** electronic or mechanical devices that enable the Cardholder or Card User to carry out payment transactions, withdraw or deposit cash into accounts, pay utility bills, check account balances, etc. Examples of terminals: POS terminals, virtual card payment acceptance terminals used in e-commerce (online), ATMs (including MBAs), ROBO terminals and imprinters.

➤ **Contactless terminal:** a terminal that enables fast transactions by simply holding a card or an NFC-enabled device (e.g. a mobile phone, smartwatch or wristband) close to the terminal. If applicable, the PIN may also need to be entered and/or the transaction receipt signed. It can be identified by the contactless symbol displayed on the terminal.

➤ **Transfond:** STFD TRANSFOND SA, the administrator and operator of the Automated Clearing House for interbank payments in Romanian lei.

➤ **Contactless transaction:** a transaction carried out at a contactless terminal. It may be carried out without entering the PIN and/or signing the transaction receipt, provided that the transaction

amount does not exceed the limits established by the card schemes or the European banking authorities. These limits are published on the Bank's website and may be changed at any time by the card organisations or the European banking authorities.

- **Token:** a unique digital string of numbers that securely replaces the card data of a card registered with a digital wallet service or enrolled on merchants' websites or applications, or in Click to Pay. A card may have one or more tokens, each uniquely associated with a specific digital wallet, device, application, merchant or the Click to Pay functionality. The token number is different from the card number, which enhances transaction security.
- **Credit transfer:** a national or cross-border payment service for crediting a payee's payment account with one or more payment transactions from the payer's payment account, based on an instruction given by the payer to the payment service provider with which the payer's payment account is held. Credit transfers include domestic and cross-border payments, as well as domestic and cross-border incoming payments.
- **Offline transaction:** a transaction carried out using a card at a terminal that allows transactions to be processed without obtaining an authorisation code from the card-issuing bank. For offline transactions, no funds are blocked, and the account is debited with the transaction amount on the settlement date.
- **User:** a natural person authorised to operate a current account or revolving account who, at the request of the account holder, is issued by the Bank with a card providing access to the funds available in that account, in accordance with Article 3.4.1.2.
- **Business day:** a day on which the Bank carries out its business activities and is open to the public, excluding Saturdays, Sundays and public holidays recognised in Romania.

### **1.3. Establishing the Relationship with the Bank. Rules Governing the Relationship**

**1.3.1.** A Client may establish a banking relationship with the Bank and obtain banking products and services through the Bank's branch network or through the remote contracting channels made available by the Bank.

**1.3.2.** For this purpose, the Client must submit the documents requested by the Bank. The Client must also complete and sign the Bank's standard forms or, where applicable, follow the Bank's standard procedures for establishing a banking relationship remotely.

**1.3.3.** The Bank shall provide the products and services requested by the Client only if the applicable eligibility criteria are met, in accordance with the Bank's policies and the applicable regulations. For certain categories of Clients (e.g. Clients opening accounts or other products remotely, minors, etc.), the Bank may impose additional conditions or restrictions. For example, basic payment accounts and accounts held by minors may only be opened through the Bank's branches and cannot be opened remotely.

#### **1.3.4. Client Representation**

In the relationship with the Bank, the Client may be represented by

- his legal representative or
- a proxy authorised under an express mandate granted by a notarised power of attorney or by means of the Bank's forms, in accordance with the applicable law and the Bank's policies on customer due diligence, anti-money laundering and counter-terrorist financing.

A mandate granted by the Client using the Bank's account proxy designation forms shall remain valid for **15 years** but may be revoked at any time. The Client undertakes to inform the authorised representative of the duration of the mandate and the rights conferred under it.

The authorisation shall remain valid until the Bank receives written or telephone notice from the Client (via MyBRD Contact) of the revocation or amendment of the mandate, or of the authorised representative's renunciation of the mandate, or until the Client's death.

If the authorised representative renounces the mandate, they must notify the account holder in advance of such renunciation.

In the event of the Client's death, the termination of the mandate shall take effect vis-à-vis the Bank from the date on which the Bank is notified of the Client's death by the submission of the death certificate or by written or oral notice given at any of the Bank's branches.

The Bank shall be entitled to request any documents it considers necessary in relation to such changes.

The Client shall be liable for any loss incurred by the Bank as a result of failing to notify the Bank of any restrictions or limitations on the authority granted to their authorised representatives, including any account proxy. In the event of a dispute concerning the appointment, scope or revocation of a mandate, the Bank may block the Account Proxy's access to the Client's account and refuse to act on any requests or instructions given by the Client's authorised representatives until the dispute has been resolved, as evidenced by documents satisfactory to the Bank.

#### **1.3.5. Clients without or with limited legal capacity**

Clients without legal capacity and Clients with limited legal capacity, and/or their legal representatives, shall comply with the legislation governing the protection of such persons when entering into legal acts, as well as with the decisions of the competent courts and authorities.

They release the Bank from any liability in respect of transactions instructed and legal acts entered into, including those that exceed the limits established by law or by a decision of the competent court or authority.

The Client and/or the legal representative shall notify the Bank and update the information and documents previously provided to the Bank immediately upon any change in the Client's legal capacity. Such changes may include, for example: the acquisition, loss or restriction of the Client's legal capacity, or the restriction or termination of the legal representative's authority to represent the Client or to consent to the Client's legal acts. The Bank shall not be liable for any loss or damage resulting from a failure to comply with these obligations.

**1.3.6.** Minors (persons under the age of 18) may obtain and use the products and services made available to them by the Bank as follows:

- those under 14 years of age – through legal representatives;
- those who have reached the age of 14 – with the consent of legal representatives, given by signing specific documents.

In certain cases, the law also requires the approval or authorisation of other persons or bodies (e.g. the family council, the guardianship court, etc.).

**1.3.7.** The legal representative of a minor Client undertakes to ensure that all transactions carried out by them on the Client's account are necessary for the minor's maintenance. Such transactions shall not exceed the scope of the legal acts that may be carried out by the legal representative without the approval of the guardianship court, the guardianship authority or the family council, as required by law, or the limits established by a decision of the competent court or authority.

**1.3.8.** The minor Client and their legal representative shall ensure that any legal acts or transactions carried out by the Client independently do not exceed those permitted under the applicable law. Currently, these are:

- for minors under the age of 14: acts of preservation; acts of disposition of low value, of an everyday nature, and performed immediately upon being entered into; and other acts expressly permitted by law.
- for minors who have attained the age of 14: acts of preservation; acts of administration that are not detrimental to the minor; acts of acceptance of an inheritance or unconditional gifts; acts of disposition of low value, of an everyday nature, and performed immediately upon being entered into.

#### **1.4. Know Your Customer. Tax Transparency Information and Reporting, CRS/FATCA. Prevention of Money Laundering and Counter-Terrorist Financing**

**1.4.1.** The Bank is required by law to verify the identity of its Clients as part of its KYC/AML procedures before establishing a business relationship or carrying out certain transactions, as well as throughout their relationship with the Bank. The Bank is also required to take measures to prevent fraud, money laundering, the financing of terrorism, tax evasion, and dealings with persons subject to international sanctions.

The Client shall cooperate with the Bank in carrying out such checks and formalities. For this purpose, the Client and the authorised representative shall provide the Bank with the requested information and documents accurately and in a timely manner and shall comply with the obligations set out in this Section 1.4. Otherwise, the Bank may:

- request additional information and documents;
- refuse or suspend transactions requested by the Client;
- block the Client's accounts and access to the contracted services/products;
- deny the Client access to new products and services; and
- terminate the contractual relationship with the Client.

The Bank may also take the measures set out in the preceding paragraph if:

- the information or documents provided to the Bank are incomplete, inconsistent or inaccurate; or
- The Bank identifies risk factors relating to • the account proxy, • the nature of the transaction or the documents supporting it, or • fraudulent activities.

**1.4.2.** The Bank may require the Client and any account proxy to provide information and supporting documents for the purpose of verifying their identity, substantiating the transaction, identifying the source of funds, the purpose and nature of the transaction, or the beneficial owner.

The Bank may request such information and documents when establishing the business relationship, opening accounts, providing services, appointing an account proxy, or for the purpose of determining the circumstances and purpose of transactions, whenever it considers it necessary, at any time during the business relationship.

The Client and the account proxy shall also provide the Bank with a specimen signature.

The Bank shall neither open nor maintain anonymous accounts (where the identity of the account holder or the beneficial owner is unknown) or accounts under fictitious names.

The appointment of an Account Proxy shall not take effect until the documents required to verify the account proxy's identity have been provided and the account proxy has submitted a specimen signature.

If the Client is represented by another person (e.g. a legal representative, an authorised representative, an account proxy, etc.), the Bank shall verify the information and documents relating to the representative's identity and the nature and scope of the representative's authority. Identity verification also applies to the beneficial owner.

#### **1.4.3. Tax information and reporting. CRS and FATCA**

**1.4.3.1.** For the purposes of FATCA and CRS reporting, the Bank is required to collect and verify certain information required under FATCA and CRS. For this purpose, when establishing the business relationship and whenever their information is updated, the Client shall provide the Bank with the FATCA and CRS information, including the Tax Identification Number (TIN) / Tax Identification Code (NIF) issued by their jurisdiction(s) of tax residence (where such a number is issued), and shall complete any declarations/forms required by the Bank for this purpose.

**NIF** means the Tax Identification Code (or its functional equivalent) assigned by the tax authorities in Romania or other countries of tax residence.

**TIN** (Taxpayer Identification Number) means the United States federal taxpayer identification number, which must be collected from US clients. For individuals, the TIN is equivalent to the Social Security Number (SSN), while for entities, the TIN is equivalent to the Employer Identification Number (EIN).

**1.4.3.2. CRS (Common Reporting Standard)** is an automatic exchange of information framework under which the Bank is required to collect and report CRS information on its Clients to the National Agency for Fiscal Administration (ANAF).

**CRS information** includes data relating to the account holder's tax status, including the NIF/TIN issued by the jurisdiction(s) of tax residence, where the Client is a Reportable Person.

A **Reportable Person** is any person who is a tax resident of a Reportable Jurisdiction and who holds accounts subject to FATCA/CRS reporting.

**CRS Self-Certification.** The Client shall provide a CRS self-certification for the purpose of establishing the CRS indicia: • upon establishing a business relationship with the Bank or opening an account and • following a change in circumstances (e.g. a change in the jurisdiction of tax residence). The self-certification includes the Client's full name, address, jurisdiction(s) of tax residence, NIF/TIN, and date of birth.

**The CRS indicia** include the following:

- the client declares a country of tax residence other than Romania;
- the Client's identity document is issued by a CRS country;
- country of domicile/residence/correspondence in a CRS country;
- a phone number or contact details from a CRS country and no phone number from Romania;
- a power of attorney or delegation of signature granted to a person with an address in a reporting jurisdiction.

**1.4.3.3. FATCA (Foreign Account Tax Compliance Act)** is the tax compliance law applicable to foreign accounts, adopted in 2010 in the United States of America (USA). Its goal is to prevent and reduce tax evasion generated by the cross-border activity of American residents.

FATCA was implemented in Romania through Law No. 233/2015 ratifying the Agreement between Romania and the United States of America to Improve International Tax Compliance and to Implement FATCA.

FATCA requires the Bank to report to ANAF information on the Bank's Clients who are Specified U.S. Persons (as defined below). ANAF then transmits this information to the US tax authorities (IRS - Internal Revenue Service).

**Specified U.S. Person (or U.S. Person)** means, in the case of an individual, a U.S. citizen (whether holding sole or multiple citizenship) and/or a U.S. tax resident who is liable to pay taxes in the United States under U.S. law, regardless of whether they reside in the United States or outside the United States.

The **indicia** that an individual may be a Specified U.S. Person are as follows:

- the customer is a US citizen or
- is a permanent resident of the USA (has a Green Card) or holds a TIN tax identification number;
- the customer has a primary/mailling address in the USA;
- the customer's place of birth is in the USA;
- the customer's phone number is from the US;
- the Client has standing instructions to transfer funds from a BRD account to the same account maintained in the United States or to the same beneficiary in the United States (at least three transfers of the same amount within a one-year period); or
- there is a currently effective power of attorney or signatory authority granted to a person with a U.S. address in respect of the Client's account.

In accordance with FATCA, a **"U.S. Reportable Account"** means a financial account maintained by a Financial Institution in Romania and held by one or more Specified U.S. Persons or by a Non-U.S. Entity controlled by one or more persons who are **Specified U.S. Persons**.

An account shall be presumed to be a financial account held by a Specified U.S. Person if at least one U.S. indicium exists in respect of at least one of the account holders and that person fails to provide evidence of their non-U.S. status in accordance with the FATCA requirements.

To confirm their FATCA status and tax residence, the Client shall submit a declaration on their own responsibility ("FATCA Self-Certification"), using the form provided by the Bank for this purpose. Where applicable, depending on the FATCA status declared by the Client, in addition to the FATCA Self-Certification, the Client shall also provide the relevant U.S. tax forms (Forms W-8/W-9).

The FATCA Self-Certification and the U.S. tax forms (Forms W-8/W-9, as applicable) must be signed and dated no later than the date on which they are received by the Bank. The FATCA Self-Certification and the U.S. tax forms (Forms W-8/W-9) may be signed either by the account holder or by any person duly authorised to sign on the account holder's behalf under a special power of attorney granted by the account holder.

The FATCA Self-Certification and the U.S. tax forms (Forms W-8/W-9) may be signed in electronic form only by means of the qualified electronic signature made available by the Bank.

A Client is considered FATCA non-compliant if they • refuse to provide the documents required to establish their FATCA status, • refuse to consent to FATCA reporting or • fail to provide, confirm or update the information requested for FATCA purposes within the prescribed time limit, despite the identification of U.S. indicia. The Bank does not establish business relationships with FATCA non-compliant Clients.

**1.4.3.4.** The Client agrees that, in order to comply with its legal obligations, the Bank may disclose to the competent authorities information concerning: • the Client's identification data; • the Client's current and future financial accounts, including the account number and the balance/value thereof; • income generated from the assets held in those accounts; • any other information required under the Fiscal Procedure Code. The authorities to which the Bank reports this information may include: (i) authorities to which the Bank is required to provide information, including tax information (for FATCA and CRS purposes); (ii) other entities that the Bank considers relevant for the purposes of FATCA and CRS in order to prevent any potential breach of these regulations; and (iii) other entities to which the Bank decides to delegate its FATCA/CRS reporting obligations, including companies within the Société Générale Group.

#### **1.4.4. Politically Exposed Persons (PEPs). Senior Public Officials**

The Bank applies enhanced customer due diligence measures to:

- Politically Exposed Persons (PEPs), their family members and persons known to be close associates of such persons. Politically Exposed Persons are individuals who are or have been entrusted with prominent public functions;
- Senior Public Officials.

The Client undertakes to provide the Bank with any additional information and documents requested by the Bank.

Details of the persons considered to be PEPs or SPOs under the applicable regulations or the Société Générale Group standards are available on the Bank's website at: <https://www.brd.ro/persoane-expuse-public>.

#### **1.4.5. Legal Residence and Tax Residence**

**The country of legal residence** is the country in which the Client has their domicile. The Client shall provide the Bank with the

legal documents establishing their domicile and, where applicable, any additional documents requested by the Bank.

**A resident is an** individual (Romanian national, foreign national or stateless person) who is domiciled in Romania.

**The country of tax residence** is the country in which an individual is liable to tax under the laws of that country.

The Client shall declare all countries of their tax residence and shall provide the Bank with documents that reasonably support such declaration.

In addition, Clients who are not tax residents shall provide the Bank with their Tax Identification Number (NIF/TIN) or its equivalent.

#### **Specific Obligations for Non-Tax-Resident Clients**

Such Clients shall provide the Bank with a certificate of tax residence if they receive from the Bank income subject to withholding tax (e.g. interest), are tax residents of a country that has concluded a double taxation treaty with Romania, and wish to benefit from the reduced tax rate provided for in that treaty. The certificate of tax residence must be:

- issued by the competent authority of the country of tax residence;
- submitted at a Bank branch before the date on which the income is received and thereafter annually, by 10 February, in the original or as a notarised copy, together with a certified Romanian translation; and
- valid on the date the income is received. For this purpose, please note that: (i) the certificate of tax residence is valid for the year in which it is submitted and for a further 60 calendar days of the following year, unless it expressly provides otherwise; (ii) in the case of interest income, the date on which the income is received is the date on which the interest is credited to the account.

#### **1.4.6. Updating data**

**1.4.6.1.** The Client shall update their personal data and the information provided to the Bank throughout the contractual relationship and shall provide the documents requested by the Bank for that purpose. This update concerns information such as:

- the identification details of the Client/Account Proxy;
- revocation of the power of attorney;
- changes affecting the Client's legal capacity;
- FATCA and CRS information (including the Client's FATCA or CRS tax residency status and NIF/TIN) etc.

**1.4.6.2.** For this purpose, the Client shall:

- notify the Bank of any changes to the information provided and submit updated versions of the documents previously provided to the Bank within five Business Days of the date of such change;
- if there are any changes affecting FATCA or CRS, provide a new valid FATCA or CRS Self-Certification, as applicable, within 90 days of such change; and
- update the information previously provided, at the Bank's request and on a periodic basis, in accordance with the Bank's customer due diligence policy and the applicable regulations.

**1.4.6.3.** Data can be updated:

- through the Bank's network of branches;
- through available remote channels (YOU BRD, brd.ro website);
- by phone, through the MyBRD Contact service (e.g.: to change correspondence data – e-mail, mailing address – or the agreement to process personal data for marketing, studies and analysis purposes).

**1.4.6.4.** The Bank shall update the Client's personal data in its records, provided that the information and documents submitted by the Client comply with the applicable legal requirements.

**1.4.6.5.** Until the Client notifies the Bank of such changes, the Bank may rely on the information in its possession as being valid. The Bank shall not be liable for any loss or damage if the Client fails to notify the Bank of such changes or fails to submit the supporting documents in a timely and secure manner.

**1.4.6.6.** If the Client fails to update their information or provides incomplete or inaccurate information or documents, the Bank may:

- refuse to carry out the requested transactions;

- block the Client's accounts and access to any of the services contracted by the Client;
- refuse to allow the Client to obtain new products and services; and
- terminate the contractual relationship with the Client.

**1.4.7.** The Bank may take any measures it considers necessary or appropriate to **prevent and combat fraud, money laundering, terrorist financing and tax evasion**, and to prevent the provision of services to persons subject to **international sanctions**. For example, the Bank:

- may request information and documents from the Client or the account proxy to verify the source of funds, the beneficiaries and the purpose of the transactions;
- investigate and suspend transactions initiated from or to the Client's account before they are processed;
- request additional investigations to determine whether a person is subject to international sanctions;
- complies with the decisions of the competent authorities regarding the implementation of international sanctions, including the freezing of funds or economic resources.

**International sanctions** are restrictions and obligations relating to the governments of certain states, non-state entities, or natural or legal persons. They are adopted by the United Nations Security Council, the European Union, other international organisations, or the United States.

Their purpose is to maintain international peace and security, prevent and combat terrorism, protect fundamental human rights and freedoms, promote and strengthen democracy and the rule of law, or pursue other objectives in accordance with the objectives of the international community or international law and European Union law.

International sanctions may include, in particular: • the freezing of funds and economic resources (see below for details of what these measures entail); • trade restrictions; • restrictions on transactions involving certain products and technologies (e.g. dual-use products/technologies, military products, etc.); • travel restrictions; • transport and communications restrictions; • diplomatic sanctions or in the technical-scientific, cultural or sporting fields.

The **freezing of funds** means preventing any transfer, access to or use of funds that would result in any change in their volume, amount, location, ownership, possession, nature or destination, or otherwise enable the use of such funds, including portfolio management.

The **freezing of economic resources** means preventing the use of economic resources to obtain funds, goods or services by any means, including by selling, hiring out, mortgaging or otherwise disposing of them.

**1.4.8. Cash Transactions.** If the Client carries out cash transactions of at least EUR 15,000 or the equivalent amount (whether in a single transaction or aggregated) during a Business Day, they shall provide the Bank with documents relating to the source of funds and the purpose of the transaction and complete a declaration identifying the beneficial owner.

**1.4.9.** The Bank reserves the right to refuse transactions carried out through the Client's accounts and to terminate its relationship with the Client if • the Client fails to provide the documents or information requested by the Bank, or provides false, incomplete or inaccurate documents or information; • BRD considers that it is unable to adequately apply customer due diligence measures for the purposes of preventing and combating money laundering; or • the Client presents to the Bank payment instruments suspected of fraud that pose payment risks or may affect settlement.

## **1.5. General Obligations, Rights and Representations of the Parties**

**1.5.1.** In addition to any other obligations assumed under this Agreement or under specific agreements, the Client shall:

**a)** Pay the Bank, in a timely manner, the charges for the products and services provided.

- These may include, as applicable: fees, interest, foreign exchange costs and other charges.
- The amounts of these charges are set out in the Fees Guide, which forms an integral part of this Agreement. It is also available at the Bank's branches, on the Bank's website at [www.brd.ro](http://www.brd.ro) and through the YOU BRD service.
- The Client may also consult the Fee Information Document at any time, which is available at BRD branches (in paper form or on another durable medium) and on the Bank's website at [www.brd.ro](http://www.brd.ro).
- The exchange rates applied by the Bank are available at the Bank's branches and on the Bank's website at [www.brd.ro](http://www.brd.ro).
- The Client who is the account holder is primarily responsible for paying all amounts due to the Bank. Only if the Client fails to fulfil this obligation may the required amounts be paid into the account by the account proxy(s) designated for that account. For this purpose, the Client who is the account holder authorises the Bank to provide the account proxy, upon request, with details of the amount and type of the applicable charges.
- The Client shall keep themselves informed on a regular basis of any changes to the Bank's fees and interest rates by consulting the Bank's branches, its website or its remote banking services.
- The Bank may charge default interest on amounts due from the Client, the total amount of which may exceed the original debt.

**b)** Comply with the Bank's business hours, as displayed at its branches.

**c)** Submit the documents requested by the Bank in the original, as a notarised copy, or in any other form required by the Bank.

**d)** During telephone calls through the MyBRD Contact service, correctly answer the questions asked by the Bank's representative for the purpose of identity verification. The Client shall provide the Bank's representative with complete and accurate information before the requested transaction is carried out or before receiving personalised information.

**e)** Behave in a respectful manner and refrain from using abusive or violent language when interacting with the Bank.

**1.5.2.** The Client understands and acknowledges that:

**a)** The Bank may submit to the Credit Bureau, the Payment Incidents Bureau and the Credit Risk Bureau (as applicable), for processing and consultation, risk information, information relating to loans, payment incidents, fraudulent activity, and discrepancies identified in the documents or declarations submitted by the Client or the account proxy(s).

**b)** The Bank may execute any instruction or authorisation given by the Client through the Bank's staff, one of its branches, a correspondent bank or another credit institution.

**c)** The authorisations and instructions given by the Client to the Bank are irrevocable unless the Parties agree otherwise in writing.

**d)** The Bank may apply preferential fees and charges to the Client:

- for specific periods, within promotions;
- based on an agreement concluded with the entity that pays the Client salaries or other monetary rights; or
- if the Client meets the eligibility conditions established by the Bank in this regard and communicated to the Client.

After • the promotional period expires, or • the agreement with the income payer ceases or no longer applies to the Client, • or the Client no longer meets the eligibility conditions to benefit from preferential costs, the Bank may charge the standard fees and charges in force at that time.

**e)** The Bank may set off any amount due and payable by the Client to the Bank against any amount owed by the Bank to the Client, regardless of the currency, the place of payment or the Bank branch through which the payment was made. If the obligations are denominated in different currencies, the Bank may, for the purpose of effecting the set-off, convert any obligation into another currency at

the exchange rate applied by the Bank on the date of the set-off in the ordinary course of its business for similar transactions. If multiple legal relationships exist between the Bank and the Client (for example, multiple accounts), and the Client wishes to set off amounts owed by each party to the other, the Client shall submit a written request to the Bank to that effect.

**1.5.3. In the case of commercially inactive Clients:**

**a)** The Bank may suspend the charging of certain fees payable by the Client, such as the current account maintenance fee, the package maintenance fee or the debit card maintenance fee, etc. If the Client becomes commercially active again, the Bank shall resume charging such fees in accordance with the Fee Guide or the relevant specific agreements; and

**b)** if the Client remains commercially inactive for an extended period, the Bank may close any account (except for a basic payment account) and any product or service linked to that account and may terminate its relationship with the Client. The Bank will notify the Client in this regard. The provisions of Article 2.39.8 shall apply accordingly.

Further details on the suspension and resumption of fee charges, the closure of products and services, and the termination of the relationship with commercially inactive Clients are available on the Bank's website (<https://www.brd.ro/tarife-si-comisioane>).

For the purposes of this Article 1.5.3:

**(i) Active Commercial Client** is the Client who meets any of the conditions listed below in points (i.1) - (i.4), cumulatively with the condition in point (i.5):

- (i.1) carries out payment transactions through any of the accounts held with the Bank (except for the payment of fees and charges due under the agreements concluded with the Bank); or
- (i.2) maintains, in any current or savings account, a balance exceeding the minimum threshold established by the Bank (or its equivalent in the currency of the account); or
- (i.3) opens a new current or savings account; or
- (i.4) has outstanding loan agreements or savings product agreements with the Bank or other BRD Group entities; and
- (i.5) has no overdue payment obligations exceeding 90 days under loan agreements with the Bank or other BRD Group entities.

**(ii) A commercially inactive Client** means a Client who does not meet the criteria for being considered a commercially active Client, as set out in point (i) above.

**1.5.4.** The Client acknowledges and agrees that any **change to the interest rate payable by the Bank and to the exchange rate** shall take effect immediately, without prior notice, if:

- it is based on a reference interest rate or a reference exchange rate; or
- it is to the Client's advantage (in which case the change may also take effect at a frequency other than that provided for in this Agreement).

The Client shall be informed of the change without undue delay by notice displayed at the Bank's branches and on the Bank's website.

**1.5.5.** The Client represents and warrants that the information contained in the documents provided to the Bank is true and accurate. The Client acknowledges that making false statements is punishable under the Criminal Code.

**1.5.6.** The Client freely consents to enter into this Agreement. The Client intends to acquire all the rights and assume all the obligations set out in these General Banking Conditions, which they consider fair and equitable. The Client confirms that the Bank has provided all the information necessary for the Client to properly understand these General Banking Conditions and all matters relating thereto.

**1.5.7.** All persons who are parties to agreements with the Bank (e.g. legal representatives, Cardholders, co-borrowers, guarantors, etc.) declare that they have received a copy of these General Banking

Conditions, are familiar with and accept their contents, and undertake to comply with their provisions.

**1.5.8.** The Client acknowledges that, in the event of exceptional changes in the circumstances underlying the establishment of the relationship with the Bank, beyond the Bank's control, the performance of the Client's obligations may become more difficult or more costly. The Client accepts the risk of such changes and undertakes to perform their obligations towards the Bank irrespective of the occurrence of such changes.

**1.6. Confidentiality**

The Bank and the Client undertake to maintain the confidentiality of all information, facts and documents relating to their relationship, except where disclosure is required by law or where the information is necessary for the resolution of disputes relating to card transactions. The Bank may disclose information subject to banking secrecy (as defined by Government Emergency Ordinance No. 99/2006) to third parties, including the National Agency for Fiscal Administration (ANAF), in the cases provided for by law or by these General Banking Conditions.

**1.7. Amendment of the Agreement**

Unless otherwise provided in this document or in specific agreements between the Client and the Bank, any amendment to this Agreement proposed by the Bank shall be communicated to the Client at least two months before it takes effect, using the agreed means of communication. The amendments shall be deemed to have been accepted by the Client unless the Client notifies the Bank in writing, before their proposed effective date, that they do not accept them.

A Client who does not agree to the amendments proposed by the Bank has the right to terminate this Agreement immediately and free of charge before the amendments take effect.

**1.8. Term and Termination of the Agreement**

**1.8.1.** This Agreement is concluded for an indefinite term. It enters into force on the date of its execution or at the time the Parties otherwise express their consent, in accordance with the law.

**1.8.2.** The Agreement may terminate either (i) in its entirety, in respect of all products and services (in which case the Client's relationship with the Bank shall also terminate), or (ii) partially, in respect of certain products and services, in which case the Agreement shall remain in force with respect to the remaining products and services.

**1.8.3.** Unless otherwise provided in this document or in specific agreements concluded between the Client and the Bank, the Agreement may terminate, in whole or in part:

- a) by agreement of the parties;
  - b) by unilateral termination by the Client:
    - at any time, with one month's notice; and, in addition,
    - if the Agreement has been concluded at a distance, by exercising the right to withdraw from the Agreement within 14 calendar days of its conclusion, without incurring any penalty.
- For termination, the Client will submit a written request to any unit of the Bank.
- Alternatively, where the Agreement has been concluded at a distance, the Client may terminate it by completing the electronic form made available by the Bank on its corporate website [www.brd.ro](http://www.brd.ro). The decision to terminate the Agreement does not need to be justified. However, the Client must first settle all amounts owed to the Bank in respect of services already provided;
- c) by unilateral termination by the Bank, with two months' notice;
  - d) by termination by the Bank, without notice, notification or other formality, in the following situations:
    - The Client has been found by the competent authorities to have engaged in unlawful activities constituting economic or financial offences or corruption offences (such as tax evasion, money laundering, the giving or receiving of bribes, etc.), and

the Bank has been notified accordingly by the competent authorities;

- in any other cases of account closure initiated by the Bank, in accordance with Article 2.39;
- e) in any other cases expressly provided for in this Agreement or in any specific agreements concluded between the Client and the Bank;
- f) in any other situations required by law or by decisions of the competent authorities, subject to prior notice to the Client.

**1.8.4.** The closure of the Client's last account held with the Bank, regardless of the manner in which it is closed, shall result in the termination of the Agreement. By way of exception, the Agreement shall remain in force after the closure of the last account if the Client also holds products or services with the Bank that are not linked to an account under specific agreements (for example, a safe deposit box).

## **1.9. Client-Bank communication**

### **1.9.1. Correspondence addressed by the Client to the Bank**

Unless otherwise provided by law or in the agreements/forms specific to the relevant products or services, any correspondence (request, notice, complaint, etc.) addressed by the Client to the Bank shall be submitted in writing by any of the following means:

- by registered mail with acknowledgement of receipt, sent to the Bank's head office (at the address specified in Section 1.1.1) or to any of the Bank's branches;
- by filling out the contact form on the website [www.brd.ro](http://www.brd.ro)/Contact section;
- by e-mail to [mybrdcontact@brd.ro](mailto:mybrdcontact@brd.ro), sent from the address with which the Client is registered in the Bank's records;
- by submitting it at any of the Bank's branches;

Where, pursuant to the law or the agreement concluded with the Bank, correspondence is required to reach the Bank within a specified time limit, it shall not be taken into consideration if received by the Bank after the expiry of that time limit.

Documents written in foreign languages must be submitted to the Bank together with their legalized translation into Romanian.

### **1.9.2. Correspondence addressed by the Bank to the Client**

Unless otherwise provided in specific agreements or by law, correspondence shall be deemed to have been delivered in the following cases:

- a) The Bank holds a copy of the correspondence, signed by the Client;
- b) the correspondence is confirmed by a shipping document issued by a courier or postal company;
- c) The client received the correspondence through alternative channels (the Bank's website [www.brd.ro](http://www.brd.ro), MyBRD Contact, telephone, e-mail, fax, SMS, YOU BRD service, etc.).

Correspondence shall be deemed properly addressed if it is sent to the last postal address, e-mail address or telephone number communicated by the Client to the Bank, according to the Contract.

### **1.9.3. Communications via MyBRD Contact**

The client can call the MyBRD Contact service to • find out information about the Bank's products and services, • request meetings with client managers, • request personalised information about the contracted products/services and • address requests related to them.

By exception, customers between the ages of 14 and 18 can only address certain types of requests to the MyBRD service. They mainly include • blocking access to remote banking services and cards, • activating, unblocking, restoring or regenerating the PIN code related to the cards, • activating or deactivating the token.

For providing certain categories of information through the MyBRD Contact service, the Bank may charge a fee, according to the provisions of the Fee Guide.

### **1.9.4. Records**

The Bank may record and store audio and video communications and electronic communications between the Client or the authorised representative and the Bank, including those conducted through the Bank's remote banking services (MyBRD Contact, MyBRD SMS, YOU BRD, etc.). The purpose is to ensure the quality of the services provided and to document the Client's requests, agreements, preferences, and the Bank's responses.

The Client confirms that they have informed the relevant persons, including any authorised representatives, about such recording and storage and have obtained their consent thereto.

The Client agrees that such recordings shall constitute admissible and conclusive evidence of the content of the recorded conversations and messages. They may be used in any judicial, extrajudicial, administrative or arbitration proceedings. The Client may refuse to have the call recorded at the beginning of the call, in which case the communication may continue through other available means.

**1.9.5. Electronic communications.** If the Client enters into a business relationship with the Bank or purchases products or services online or at a distance, the following shall constitute valid evidence and may be used in any judicial, extrajudicial or administrative proceedings:

- a) electronic communications sent by the Bank to the Client during the process of establishing the business relationship/contracting (including by SMS, email, displayed electronic messages, electronic documents made available on web pages, etc.);
- b) the options, requests and communications submitted by the Client by electronic means, in accordance with the procedure communicated by the Bank (e.g. by completing or selecting fields on dedicated web pages, by email, etc.); and
- c) audio and video recordings made during the process of establishing the business relationship with the Bank or entering into the relevant agreement.

**1.9.6.** Communication between the parties shall be carried out in **Romanian**.

### **1.10. Force Majeure**

Neither the Bank nor the Client shall be liable for any losses caused by force majeure. Force majeure means any unforeseeable, unavoidable event beyond the control of either Party that renders it absolutely impossible for that Party to perform all or part of its contractual obligations (e.g. natural disasters, strikes, war).

The Party affected by the force majeure event must notify the other Party by telephone or fax within five calendar days. Within the following 15 calendar days, the affected Client must provide the Bank with a force majeure certificate issued by the competent authorities, either by registered mail with acknowledgement of receipt or by submitting it at any of the Bank's branches.

### **1.11. Governing Law. Disputes. Language**

**1.11.1.** The relationship between the Bank and the Client shall be governed by **Romanian law**. The Bank also applies the regulations of the Société Générale Group (of which the Bank is a member), including those relating to customer due diligence, the prevention of money laundering and terrorist financing, and the implementation of international embargoes and sanctions.

**1.11.2.** This Agreement is written in **Romanian**.

**1.11.3.** Any dispute will be resolved amicably by the parties. If this is not possible, it will be resolved by the competent court.

**1.11.4. Extrajudicial proceedings.** If the Client considers that their rights have been infringed, they may also refer the matter to:

- a) National Authority for Consumer Protection. Its address is: Bucharest, Blvd. Aviatorilor no. 72, sector 1. Additional information is available on the website [www.anpc.ro](http://www.anpc.ro), where the Client can fill in an online complaint form;
- b) Alternative Banking Dispute Resolution Centre (CSALB). It is an autonomous legal entity, non-governmental, politically independent, non-profit and serving the public interest. Its purpose is to ensure that consumers of banking services have

access to alternative dispute resolution procedures in disputes with credit institutions. The CSALB headquarters is in Bucharest, Str. Sevastopol nr. 24. Sector 1. Details are available at phone number (021) 9414 and on the website [www.csalb.ro](http://www.csalb.ro);

- c) mediation proceedings, in accordance with Law No. 192/2006;
- d) National Bank of Romania, headquartered at str. Lipscani nr 25, sector 3, Bucharest, 030031. Additional information is available on the website [www.bnr.ro](http://www.bnr.ro).

The addresses and contact details of the entities mentioned above are those as of the date of conclusion of the Agreement. The Bank shall not be liable for any subsequent amendments thereto.

**1.11.5.** If the Client submits a complaint regarding payment services, the Bank shall respond in writing within 15 business days of receipt of the complaint. If, in exceptional circumstances, the Bank is unable to respond within that period for reasons beyond its control, it shall send the Client a holding reply indicating the maximum time limit within which the final response will be provided. The time limit for the final response shall not exceed 35 business days.

## **2. ACCOUNTS AND PAYMENT SERVICES – GENERAL RULES**

**2.1. Account types.** At the Client's request, the Bank opens various types of accounts in RON or foreign currency, such as: payment accounts (current accounts/basic current accounts, with or without linked debit cards; revolving accounts with linked credit cards); deposit accounts; and savings accounts.

The Client may request that products and services be linked to these accounts, subject to the conditions communicated by the Bank.

**2.2. Technical accounts.** The Bank may maintain, in its records, technical accounts allocated to the Client, to be used exclusively for technical administrative purposes relating to:

- measures restricting the disposal of funds (e.g. garnishments, precautionary measures, etc.);
- certain transactions carried out or requested by the Client, such as: crediting accounts, extending the due date of a payment obligation, collecting insurance premiums or amounts due to the Bank.

The opening of technical accounts does not create any rights or obligations between the Parties in addition to those arising from the accounts opened by the Client. The provisions of the Agreement relating to accounts do not apply to technical accounts.

**2.3. PISP/AISP.** The Client has the right to use payment initiation services and account information services. For online-accessible accounts, the Bank grants access to payment initiation service providers (PISPs) and account information service providers (AISPs) on an objective, non-discriminatory and proportionate basis. Details can be found in section 3.5 (Remote banking services).

**2.4. Minimum Available Balance.** Certain products and services require a minimum amount to be maintained either in the account to which the product or service is linked or, as applicable, in any of the Client's accounts. If the Client fails to maintain the required minimum amount by the end of the day on which they subscribed to the products or services, such products or services shall be cancelled automatically. If the Client has other outstanding payment obligations, the available funds in the account(s) shall first be applied towards the settlement of those obligations. The requested products or services shall then be established, provided that the required minimum amount remains in the account(s).

**2.5. Changing accounts.** If the Client requests the account switching service, the Bank (acting as the receiving bank) shall open a current account in accordance with the terms set out in Section 3.6 below.

### **2.6. Account proxy**

The Client, as the account holder, may appoint Account Proxies for any of their accounts held with the Bank. For this purpose, the

Client must complete the forms made available by the Bank or submit a power of attorney authenticated by a public notary, expressly specifying the powers granted to the Account Proxy.

For accounts opened online or remotely, the Bank may restrict the appointment of an Account Proxy at the time the account is opened. In such case, the Client may subsequently visit any of the Bank's branches to appoint an Account Proxy. The Account Proxy shall at all times act solely in the name and on behalf of the Client who is the Account Holder.

### **Rights of the Account Proxy**

The account proxy **designated in the Bank forms** has the following rights:

- a) to carry out transactions on the accounts for which they have been appointed as Account Proxy, including by means of electronic payment instruments – cards and remote access payment instruments, such as Internet Banking/Mobile Banking (unless otherwise provided in the relevant agreements);
- b) to place deposits from the current account in the name of the Client who is the Account Holder. The same persons who are appointed as Account Proxies for the relevant current account shall also be appointed as Account Proxies for such deposits;
- c) to close the Account Holder's deposits opened through the relevant current account and to close the related savings accounts, but only if they have been appointed as the Account Proxy for those deposits or savings accounts;
- d) to request personalised information about the products held by the Account Holder, including account statements for the period during which they act as the Account Proxy. Such account statements shall include all transactions carried out on the account during that period;
- e) to request that the account be blocked in the event of suspected fraud through the MyBRD Contact service. The account may be unblocked only at the request of the Account Holder, at any of the Bank's branches or through the MyBRD Contact service.

When opening a deposit, the Account Holder may appoint Account Proxies for the deposit account. Any Account Proxy appointed for the deposit account shall also be appointed as the Account Proxy for the current account linked to the deposit.

### **Restrictions Applicable to the Account Proxy**

An Account Proxy **appointed using the Bank's forms** may not perform the following transactions on behalf of the Account Holder:

- a) opening or closing current accounts;
- b) opening savings accounts;
- c) applying for loans;
- d) the appointment or revocation of other proxies;
- e) to redeem deposits opened from a current account for which no Account Proxy has been appointed;

Such transactions may only be carried out under an express notarised power of attorney.

The powers of the Account Proxy shall remain valid only for as long as they act as the Account Proxy, regardless of whether they were appointed using the Bank's forms or under a notarised power of attorney.

The provisions of Article 1.3.4 shall also apply to the Account Proxy. (Client Representation).

**2.7.** Any transaction (e.g. intra-bank/interbank payments, bill payments, foreign exchange transactions, collections, cash deposits and withdrawals, etc.) instructed by the Client or the Account Proxy shall be carried out through the current account.

**2.8.** To carry out payment transactions, the Client shall use the forms and payment instruments made available by the Bank.

**2.9.** The Bank shall determine the banking route used to execute credit transfer transactions, including through correspondent banking relationships.

**2.10.** The execution of international funds transfers may involve multiple institutions. Accordingly, in addition to the payment service provider of the transfer originator (which receives the

payment instruction from the originator) and the payment service provider of the transfer beneficiary (which receives the funds), the following may also be involved:

- correspondent bank: a bank with direct access to the international interbank network, which facilitates international funds transfers that another bank is unable to execute directly; and (where applicable)
- one or more intermediary banks.

**2.11.** For incoming interbank credit transfers in foreign currency, the Client beneficiary's account shall be credited in the currency specified in the payment instruction. If the two currencies do not match, the Bank shall convert the amount into the currency of the beneficiary's account using its exchange rate applicable on the transaction date, as communicated to the Client in the account statement.

**2.12.** For incoming interbank credit transfers in RON, the currency specified in the payment instruction must match the currency of the beneficiary's account. If they do not match, the Bank shall reject the payment instruction.

**2.13.** For intra-bank transfers in foreign currency between different clients of the Bank, the currency specified in the payment instruction must match both the beneficiary's account currency and the payer's account currency. If they do not match, the Bank shall reject the payment instruction.

**2.14.** The account credited shall always be the account specified in the payment instruction.

**2.15.** The Bank shall not be liable for delays in the execution of incoming foreign currency credit transfers that cannot be processed due to non-compliance with national or international regulations.

**2.16.** The Bank reserves the right to deduct its fee from any amount received before crediting the Client's account. The Client shall be informed of the total amount of the payment transaction and the applicable fee through the account statement.

**2.17.** For interbank credit transfers in foreign currency, the payer's account shall be debited in the currency specified in the payment instruction. If the two currencies do not match, the Bank shall convert the amount into the currency of the account to be debited using its exchange rate applicable on the transaction date, as communicated to the Client in the account statement.

**2.18.** Before executing the payment, the Bank may request supporting documents to verify the purpose of the payment, in accordance with the applicable legal requirements.

**2.19.** If the Client requests a cash withdrawal from a foreign currency account in an amount of less than EUR 5, USD 5 or the equivalent of 5 units of another currency, the amount shall be converted into RON at the Bank's exchange rate applicable on that day and paid to the Client in RON.

**2.20.** The Bank shall be entitled, without the Client's (or the Client's heirs') prior consent or prior notice:

- a) to correct amounts or transactions incorrectly recorded in the Client's account due to a Bank error (e.g. transactions executed twice or multiple times, or otherwise incorrectly executed by the Bank), so as to restore the account balance to the correct position, as if the error had never occurred;
- b) to debit the Client's account and refund to the payer, in whole or in part, any amount credited to the Client if the payer's payment service provider notifies the Bank (including through secure interbank channels, e.g. SWIFT messages) that the payment transaction was executed incorrectly due to an error on the part of the payer's payment service provider (e.g. the transaction was executed twice or multiple times, or was otherwise executed incorrectly);
- c) to debit the Client's account and refund to the payer, in whole or in part, any amount credited to the Client in the event of fraud or suspected fraud identified or reported, including through secure interbank channels (e.g. SWIFT messages). In such cases, the Bank may take any measures it considers appropriate

to prevent or limit the consequences of actual or suspected fraud, including, for example, blocking the relevant funds in the account, blocking the account and/or the related payment instruments (cards, Internet Banking and Mobile Banking services, etc.), including until an official communication is received from the competent authorities, where applicable;

- d) to make payments from the Client's accounts (except for the revolving account) based on final and enforceable court judgments or arbitral awards, or other enforceable titles, at the request of the persons or entities entitled thereto;
- e) if the Client receives pensions, disability benefits or other similar benefits, allowances, incentives or other social benefits into the account, the Bank may, at the request of the paying institution, retain any amounts erroneously credited to the Client's account, including after the Client's death, and refund such amounts to the paying institution. Any disagreement or dispute relating to such refunds shall be settled between the Client (or the Client's heirs) and the paying institution, without any involvement of the Bank.

The Bank shall not be liable to compensate the Client for any corrections or transactions carried out in accordance with points (a) to (e) above. Under these General Banking Conditions, the Bank shall be deemed to be authorised by the Client to carry out such corrections and transactions.

**2.21.** The Bank may set limits and thresholds for payments made using various payment instruments.

**2.22.** Payment transactions carried out using debit instruments shall be governed by the applicable legislation on cheques, bills of exchange, promissory notes and the Payment Incidents Register. The debit instrument payment transactions offered by the Bank are listed in the Fees Guide. The Client must ensure that sufficient funds are available in the account to cover payment of the issued debit instruments: (i) on the date of issue, in the case of cheques, and (ii) on the due date, in the case of bills of exchange and promissory notes.

**2.23.** In the event of an unauthorised overdraft, the Bank may, from the date on which the overdraft is recorded in the account, charge default interest on the debit balance of the account, in accordance with the Fees Guide.

**2.24.** For foreign exchange transactions between the Client's accounts held with the Bank, the Bank shall convert the amount into the currency of the account to be credited using its exchange rate applicable on the transaction date, as communicated to the Client in the account statement. Any foreign exchange request submitted by the Client shall be irrevocable once made by signing a foreign exchange order or a transaction-specific agreement, regardless of whether settlement is to take place on the same day or on another value date.

**2.25.** The Client shall bear all costs arising from exchange rate differences. Furthermore, if the Client fails to comply with or modifies the instruction submitted to the Bank, the Client shall bear all resulting consequences (including losses and any additional costs incurred by the Bank).

**2.26.** Where a transaction is carried out under a specific agreement concluded with the Bank, any dispute relating to that transaction shall be subject to the complaint period provided for in the relevant agreement.

**2.27.** The Client shall be kept informed through BRD's communication channels of any payment service unavailability and the estimated time for service restoration.

#### **2.28. Automatic Account Debiting**

The Client irrevocably and unconditionally authorises the Bank, without prior notice, to debit any account held or to be opened by the Client with the Bank for any amounts due and payable to the Bank or for services provided by the Bank under a mandate, if the account specified in the relevant agreement does not contain sufficient funds. Such amounts may include, for example, fees, charges, interest,

default interest, amounts representing an unauthorised overdraft, loan-related costs, insurance premiums, etc.

This authorisation grants the Bank the right, but not the obligation, to debit the Client's accounts in accordance with the preceding paragraph.

The Bank may also carry out any foreign exchange transactions necessary to recover such amounts in the currency in which they are payable. For this purpose, the Bank shall use its exchange rate applicable to card transactions in effect on the date of the foreign exchange transaction.

For automatically renewable term deposits, any amounts due from the Client shall be debited on the maturity date of the term deposits, after which the term deposits shall be renewed for the reduced amount.

The Client shall not be exempt from default charges on the amounts due or from being reported to entities that collect creditworthiness information. According to art. 2030 Civil Code, in the event of the Client's death, the authorisation granted to the Bank under this Article 2.28 shall remain valid for the performance of successive acts forming part of an ongoing activity of a continuous nature (e.g. the collection of monthly loan repayments). However, the parties and their heirs shall be entitled to revoke the authorisation or waive it.

## **2.29. Information Required for the Execution of a Credit Transfer Payment Order**

**2.29.1.** The **Client acting as payer** must include the following information in the payment order:

### **2.29.1.1. For domestic credit transfer payments:**

- a) the name and account number of the Client acting as payer (the Bank account in IBAN format);
- b) the name/denomination and account number of the Client acting as beneficiary (in IBAN format);
- c) payment amount;
- d) date of issue of the payment order (day, month, year). It must be unique, feasible and definite.

In addition, for payments **to the State Treasury**, the Client shall also provide:

- (i) the tax identification code of the Client acting as payer and the Client acting as beneficiary;
- (ii) the payment reference number assigned by the National Agency for Fiscal Administration (ANAF);
- (iii) the payment order number given by the paying Client;
- (iv) references relating to the economic purpose of the transaction.

### **2.29.1.2. For international credit transfers:**

- a) Paying Client name;
- b) IBAN code of the paying client;
- c) payment amount;
- d) transfer currency;
- e) Beneficiary's name and full address – for payments outside the European Economic Area (EEA);
- f) the unique identification code of the beneficiary's account (in IBAN or non-IBAN format);
- g) the name and address of the beneficiary's payment service provider, or its BIC, for payments outside the European Union (EU) / European Economic Area (EEA). If both the name and the BIC are provided, the Bank shall use only the BIC for transmitting the payment;
- h) date of issue – it must be unique, valid and definite;
- i) charges section. This indicates how charges are to be borne for foreign currency payments and RON payments to accounts held with banks abroad. It shall be completed with the code OUR, BEN or SHA, according to the Client's choice, as follows:

- "OUR" – all charges relating to the payment shall be borne by the payer (including any charges of intermediary banks);

- "BEN" – all charges relating to the payment shall be borne by the beneficiary (including any charges of the intermediary bank(s));
- "SHA" – the Bank's charges shall be borne by the payer, while the charges of the intermediary bank(s) and the beneficiary's bank shall be borne by the beneficiary.

**2.29.1.3.** For international foreign currency payments to beneficiaries holding accounts with banks in the European Union (EU) or the European Economic Area (EEA), the applicable charging option is SHA. For such payments, the Bank reserves the right to change the charging option selected by the payer if it is other than SHA.

**2.29.2.** Before initiating a credit transfer, the **Client acting as the beneficiary** shall provide the payer with the name of the Client holding the account and the Unique Identification Code (the account number in IBAN format). The Client shall inform the payer that only the account holder may be designated as the beneficiary of the payment, and not the authorised representative. Otherwise, the Bank may refuse to execute the payment.

**2.29.3.** The Bank shall not be liable for any failure to perform, delay in performing or improper performance of its obligations under the Agreement resulting from the acts or omissions of third parties (correspondent banks, agents, etc.) or from other causes not attributable to the Bank.

**2.29.4.** The Bank shall not be liable where the Client has provided incorrect or incomplete information resulting in the non-execution, delayed execution or defective execution of the payment transaction. In such cases, the Bank shall make all reasonable efforts to recover the funds involved. The Bank may charge the Client a fee for the recovery operation, in accordance with the Fees Guide.

## **2.30. Authorisation of Credit Transfer Payment Transactions**

**2.30.1.** Payment transactions initiated by the Client must be authorised by the Client or by the authorised representative, in the manner provided for in the Contract.

**2.30.2.** Where consent is given by means of a handwritten signature, the signature must match the specimen signature lodged with the Bank.

**2.30.3.** The Bank is entitled to rely on the authenticity, accuracy and genuineness of the signatures appearing on the instructions submitted to the Bank.

**2.30.4.** The Bank shall not be liable for any consequences arising from the fraudulent or improper use of signatures or Personalised Security Credentials, or from failure to comply with the payment transaction authorisation procedures agreed in the Contract.

## **2.31. Receipt and Acceptance of a Credit Transfer Payment Order**

**2.31.1.** A payment order shall be deemed to have been received by the Bank at the time it is received, if it is received on a Business Day before the applicable cut-off time (where such a cut-off time applies to the relevant transaction). The cut-off times for payment order operations are published on the website [www.brd.ro](http://www.brd.ro) and in BRD branches.

**2.31.2.** Where the payer and the Bank agree that execution of the payment order is to commence on a specific day, the payment order shall be deemed to have been received on the day agreed between the Bank and the Client.

**2.31.3.** Payment orders received after the applicable cut-off time or on a non-Business Day shall be deemed to have been received on the next Business Day.

**2.31.4.** Payment orders are considered received as follows:

- a) those on paper: on the date on which they are presented at the Bank's branch, mentioned on the form signed by the Bank;
- b) those submitted through remote banking services: when the Client gives consent in accordance with the Contract.

**2.31.5.** A payment order shall be deemed to have been accepted by the Bank if it has been received and verified as valid.

**2.31.6.** A payment order shall be deemed valid if all of the following conditions are met:

- a) it has been completed with all the information required for its execution;
- b) is authorised under the Contract; and
- c) the payer's current account specified by the Client contains sufficient funds to execute the payment and pay the applicable charges.

**2.31.7.** The Bank shall debit the current account with the amount of the payment order after it has been accepted. By way of exception, where the Client and the Bank agree that execution of the payment order is to commence on a specific day, the Bank shall debit the account at the agreed time of execution.

### **2.32. Refusal of Credit Transfer Payment Transactions**

**2.32.1.** The Bank may refuse to execute a payment transaction and may take any measures it deems necessary, including cancelling or blocking the payment instrument, if:

- a) The Client fails to comply with the provisions of the Contract (e.g. fails to ensure that sufficient funds are available in the account, the payment order does not contain all the required information, is unclear, or contains erasures, cross-outs or overwriting, etc.);
- b) The Client fails to provide the information or supporting documents requested by the Bank;
- c) the payment transaction may violate applicable legal requirements;
- d) the Client's account is subject to an attachment, seizure or any other similar measure;
- e) there are suspicions of fraudulent or potentially fraudulent activity, money laundering or terrorist financing;
- f) the Client instructs the Bank to make a payment to an entity subject to international sanctions;

**2.32.2.** A payment order refused by the Bank shall be deemed not to have been received by the Bank.

**2.32.3.** The Bank shall notify the Client, without undue delay, of the refusal to execute a payment order and, where possible, of the reasons for such refusal. The notification shall be sent by telephone, e-mail, SMS or via the YOU BRD service. The notification shall also include the procedure for rectifying the errors that led to the refusal, except where the provision of such information is prohibited by law.

**2.32.4.** Where the refusal is objectively justified, the Bank may charge a specific fee in accordance with the Fees Guide.

### **2.33. Revocation of Credit Transfer Payment Orders**

**2.33.1.** The payer may not withdraw consent to a payment transaction after the payment order has been received and accepted by the Bank.

**2.33.2.** By way of exception, the Client may revoke a payment transaction where the parties have agreed that its execution is to commence on a specific day (e.g. a direct debit or a scheduled payment order), provided that the revocation is communicated no later than the end of the Business Day preceding the agreed debit date.

**2.33.3.** The Client may withdraw consent to the execution of a series of payment transactions (e.g. direct debits, scheduled payment orders, etc.). Once consent has been withdrawn, any subsequent payment transaction shall be deemed unauthorised.

**2.33.4.** The withdrawal of consent shall be made in writing (by fax, e-mail or letter). If it is communicated by any other means, the Client shall also submit the request to the Bank in writing no later than the end of the Business Day preceding the agreed debit date. Otherwise, the Client shall be liable for any loss suffered by the Bank.

**2.33.5.** Where the Client revokes the payment after giving consent, the Bank shall take the necessary steps to revoke it. If the payment has already been transmitted to the beneficiary's bank or has already been credited to the beneficiary's account, it may be revoked only

with the beneficiary's consent. The Bank shall not be liable if the beneficiary does not consent to the return of the funds. The Bank may charge a specific fee for revoking a payment after consent has been given, in accordance with the Fees Guide.

### **2.34. Execution of Credit Transfer Payment Orders**

**2.34.1. Terms.** The maximum time within which the Bank executes a payment transaction (by crediting the payment account of the beneficiary's payment service provider) depends on the type of payment transaction, the cut-off time for receipt of the payment order by the Bank and the time at which the payer's account is debited.

The Bank shall execute payment transactions within the time limits set out below. "T" means the date on which the Bank receives the payment order:

- a) for **domestic payments**: no later than T+1;
- b) for **cross-border payments**:

- no later than T+1 for payments in euro or another currency where the beneficiary's payment service provider is located in the European Union or the European Economic Area;
- no later than T+2 for payments in any currency where the beneficiary's payment service provider is located outside the European Union and the European Economic Area.

When calculating these time limits, non-Business Days and non-banking days (in Romania and other countries) shall not be taken into account.

**2.34.2.** The Bank shall not be liable for any delay in meeting these time limits due to the external banking system, requests by the Bank or correspondent banks for information or supporting documents, time zone differences, or any other causes beyond the Bank's control.

### **2.35. Liability**

**2.35.1.** The Bank shall execute a credit transfer payment order based on the beneficiary's Unique Identifier (in IBAN or non-IBAN format) provided by the payer.

If the Unique Identifier provided to the Bank is incorrect, the Bank shall not be liable for the non-execution or defective execution of the payment transaction. However, the Bank shall make reasonable efforts to recover the funds involved. If recovery of the funds is not possible, the Bank may, at the Client's written request, provide the Client with the relevant information in its possession to enable the Client to initiate legal proceedings to recover the funds.

**2.35.2.** Where the Client requests recovery of the funds as a result of the Client's error, the Bank may charge a fee for the recovery operation in accordance with the Fees Guide.

**2.35.3.** Where a non-executed or defectively executed payment transaction is reported by the Client, the Bank shall immediately investigate the payment transaction and inform the Client of the outcome, regardless of whether or not it is liable.

**2.35.4.** For payment transactions initiated by the payer, where the payer notifies the Bank of an unauthorised or incorrectly executed payment transaction, the following shall apply:

- The Bank shall immediately refund the Client the amount of the payment transaction, and in any event no later than the end of the following Business Day. The Bank shall restore the Client's account to the state in which it would have been had the payment transaction not been executed, regardless of whether it was initiated directly by the payer or through a payment initiation service provider (PISP).
- By way of exception, the Bank shall not be liable if it can prove that the beneficiary's payment service provider received the amount of the payment transaction within the execution time agreed with the Client. In such case, the beneficiary's payment service provider shall be liable to the beneficiary and shall immediately make the amount of the payment transaction available to the beneficiary.

**2.35.5.** For payment transactions initiated by or through the beneficiary, the Bank shall be liable to the beneficiary for the correct transmission of the payment order to the payer's payment service provider. The Bank shall ensure that the amount of the payment

transaction is made available to the beneficiary immediately after the funds have been credited to the Bank's account.

**2.35.6.** The Client undertakes to indemnify the Bank against any loss, damage or expense arising from the Client's breach of the Contract. The Client shall also indemnify the Bank where the Client is held financially liable for refused payment transactions, within the limits provided by law.

**2.35.7.** In relation to losses arising from unauthorised payment transactions carried out using lost, stolen or misappropriated payment instruments:

- The payer's liability shall be limited to EUR 30 or the equivalent amount in RON, provided that the payer (i) did not act fraudulently and (ii) did not intentionally breach the obligations relating to the issuance and use of the payment instrument (including the obligation to notify the Bank of its loss, theft or misappropriation).
- The payer shall bear the full amount of such losses (the limit referred to in the preceding paragraph shall not apply) where the losses result from fraud or from the payer's intentional or grossly negligent breach of the obligations imposed by law and the Contract.

**2.35.8.** If the Bank is found to be liable for the non-execution, defective execution or delayed execution of a payment transaction, it shall also be liable, in accordance with the law, for any interest or fees incorrectly charged to the Client.

#### **2.36. Security Requirements and Corrective Measures**

**2.36.1.** The Client shall keep the personalised security credentials of the payment instruments used to authorise payment transactions secure.

**2.36.2.** The Bank shall ensure that the personalised security credentials of the payment instrument are not accessible to any person other than the Client authorised to use that payment instrument.

**2.36.3.** The Client shall use the payment instruments in accordance with the law and the contract governing their use.

**2.36.4.** The Client shall notify the Bank in the event of the loss, theft or unauthorised use of the payment instrument. The notification shall be made without undue delay, within the time limits and under the conditions set out in the Contract, through the MyBRD Contact service or by any other specific means agreed with the Bank.

**2.36.5.** The Bank may block the payment instrument for reasons relating to its security, where there is suspicion of unauthorised or fraudulent use, or where there is a significantly increased risk that the payer may be unable to fulfil its payment obligation.

**2.36.6.** The Bank shall inform the Client of the blocking of the payment instrument and the reasons for it before the payment instrument is blocked, where possible, or immediately afterwards, unless providing such information is not possible for objectively justified security reasons or is prohibited by law.

**2.36.7.** The Bank shall unblock the payment instrument or replace it once the reasons for blocking no longer exist.

#### **2.37. Refunds for Payment Transactions Initiated by or Through the Beneficiary**

**2.37.1.** The payer may request that the Bank refund an authorised payment transaction initiated by or through the beneficiary (i.e. a direct debit) that has already been executed, if all of the following conditions are met:

- a) the refund is requested within eight weeks of the date on which the funds were debited;
- b) at the time consent was given, the authorisation did not specify the exact amount of the payment transaction;
- c) the amount of the payment transaction exceeded the payer's reasonable expectations, taking into account the payer's previous spending pattern, the terms of the Contract and other relevant circumstances; and

d) The payer shall, at the Bank's request, provide relevant information demonstrating that the above conditions are met.

**2.37.2.** Within 10 Business Days of receiving the refund request, the Bank may either refund the full amount of the payment transaction or provide a reasoned refusal of the refund, in accordance with the law.

**2.37.3.** The payer shall not be entitled to a refund where:

- the payer gave consent to the payment transaction directly to the Bank; and
- (where applicable) the Bank or the beneficiary provided or made available to the payer, in the agreed manner, information on future direct debit transactions at least four weeks before the due date.

#### **2.38. Evidence of Payment Transactions, Account Statements and Fee Statements**

**2.38.1.** The Parties agree that the Client shall be informed of the transactions carried out on the account by means of the account statement. The account statement contains the details required for each payment transaction, including: • its unique reference, • the beneficiary (when the Client orders a payment), or the payer (when the Client collects an amount), • the amount of the payment transaction, • the price charged by the Bank, • the exchange rate (if applicable), • the value date of the debit/credit of the account, etc.

**2.38.2.** The account statement shall be made available to the Client free of charge, in paper form, at the Bank's branches: (i) once a month, for current and savings accounts, and (ii) once per billing cycle, for revolving accounts linked to credit cards. In addition:

- at the account holder's request made by telephone (through the MyBRD Contact service), the Bank shall send account statements covering up to the 12 months preceding the request by e-mail to the e-mail address recorded in the Bank's records.
- Specific agreements or other contractual documents may provide for other methods of making account statements available.

**2.38.3.** At the request of the Client or an authorised signatory on the account, the Bank may, subject to the fee set out in the Fees Guide:

- provide other information relating to payment transactions in addition to that included in the account statement;
- provide information on payment transactions at a different frequency or by means other than those referred to above;
- issue additional account statements or transaction listings (for days on which transactions were recorded on the account) at any of the Bank's branches, within a maximum of 72 hours of the request.

**2.38.4.** The Client may report any unauthorised or incorrectly executed payment transaction debited from the Client's account by submitting a written complaint at any of the Bank's branches, as soon as possible and without undue delay (and no later than two months from the date on which the account was debited, as shown in the account statement). Claims submitted after this period may be considered by the Bank only where the delay is justified and the claim is submitted no later than 13 months from the date on which the account was debited.

**2.38.5. Statement of Fees.** The Bank shall make available to the Client, free of charge, a Statement of Fees covering all fees incurred during the preceding 12 completed months, at least once a year, in paper form, at the Bank's branches. For payment accounts, the Statement of Fees shall also indicate, for the relevant period, where applicable:

- the interest rate applicable to the overdraft facility and the total amount of interest charged in respect of the overdraft facility;
- the credit interest rate and the total amount of credit interest accrued on the funds held in the payment account.

#### **2.39. Closing accounts**

##### **2.39.1. Closing accounts at the Client's request**

The account may be closed, at the Client's request, under the following conditions:

- a) The request must be submitted to the Bank in writing, signed.

- b) Before closing the account, the Client shall pay all amounts owed to the Bank.
- c) The account must not have any active products/services attached. Before the account is closed, the Client must terminate or otherwise settle the status of any products or services linked to it.
- d) If there are debit or credit cards attached to the account, the account will be closed 30 calendar days after all these cards are cancelled or blocked.
- e) If the account is seized, the Bank is obliged to refund to the Client only the amounts exempt from seizure, according to the law.
- f) If the account or the funds held in the account are subject to precautionary measures imposed by the criminal investigation authorities or the criminal courts, the account may be closed only after the Bank receives the written approval of those authorities, issued at the Client's request.

#### **2.39.2. Death of the Client**

The Client's death may be notified to the Bank by any interested person. The person shall also provide supporting documents, such as a death certificate, certificate of inheritance, certificate of legacy, deed of partition, court judgment, a letter issued by a notary's office or law firm regarding the determination of the Client's estate, or a letter issued by another institution.

The Bank may also become aware of the Client's death through other means, such as publicly available sources or other media.

If the Bank becomes aware of the Client's death, by whatever means, it shall be entitled to block the Client's accounts. The funds held in the accounts shall be released only to the heirs designated in the certificate of inheritance. They shall also provide supporting documents, including identity documents, the death certificate and documents evidencing their status as heirs.

If there is more than one heir, until the estate has been partitioned, the Bank may release the funds held in the accounts only with the consent of all heirs, in accordance with Article 2187(1) of the Romanian Civil Code.

#### **2.39.3. Closing accounts at the Bank's initiative**

The Bank shall be entitled to close any of the Client's accounts, except for a basic payment account, without prior notice or any notice period, in any of the following cases:

- a) the following conditions are cumulatively met:
  - the account balance (or its equivalent in the account currency) is at or below the minimum threshold communicated by the Bank;
  - no payment transactions have been carried out on the account for an extended period; and
  - no products or services are linked to the account. Further details are available on the Bank's website at <https://www.brd.ro/tarife-si-comisioane>.
- b) The Client delays or refuses to provide the documents requested by the Bank or any amendments thereto;
- c) two payment default incidents are recorded;
- d) The Client fails to provide supporting documents relating to the payment transactions or provides documents that are unsatisfactory;
- e) The Client fails to comply with the obligations assumed under the Contract, including, for example, those relating to customer due diligence, CRS and FATCA, anti-money laundering and counter-terrorist financing (as set out in Section 1.4), those set out in Section 1.5 (General Obligations, Rights and Representations of the Parties), Art. 2.40.3. 3.4.2. (Security Requirements and Notifications in the Event of Unauthorised Card Use), art. 3.5.1.5.4. (Subscriber's Obligations), art. 3.5.3.9. (Other obligations of the Subscriber), ANNEX – Information on the Processing of Personal Data etc.;

- f) the business relationship or the Client poses risks that are unacceptable to the Bank, the BRD Group or the Société Générale Group;
- g) the Client's conduct is inappropriate or abusive towards the Bank's employees, thereby affecting the Bank's reputation or the physical or psychological integrity of its employees.

#### **2.39.4. Closure of Basic Payment Accounts**

By way of exception to the provisions of the preceding Article, a basic payment account may be closed unilaterally by the Bank only if one of the following conditions is met:

- a) The Client has deliberately used the account for unlawful purposes;
- b) no transactions have been carried out on the account for more than 24 consecutive months;
- c) The Client has provided inaccurate information in order to obtain the account, and the correct information would not have entitled the Client to obtain it;
- d) The Client is no longer lawfully resident in the European Union;
- e) The Client subsequently opens a payment account with another credit institution in Romania that provides access to the services associated with a basic payment account.

**2.39.5.** Upon the closure of the current account, regardless of the manner in which it is closed, all agreements relating to the payment services linked to that account shall terminate (including, for example, direct debits, standing orders and future-dated payment orders).

**2.39.6.** Following the full repayment of a loan or the closure of a deposit, if the Client wishes to close the current account linked thereto, the Client shall express that intention by completing the Bank's relevant forms.

**2.39.7.** Until the account is actually closed, the Client shall regularise the funds held in the account. To do so, the Client may transfer the funds to another account or withdraw them in cash.

If the Client does not choose either of these options before the account is actually closed, the funds remaining in the account on the date of closure shall be held in an account maintained by the Bank and kept at the Client's disposal. In such case, any subsequent withdrawal of the funds shall be subject to the fees set out in the Fees Guide in force on the date of withdrawal. From the date of closure of the account, no credit interest shall accrue on such funds.

**2.39.8.** If the account is closed at the Bank's initiative, the Client's (or the Client's heirs') right to claim the funds held in the account on the date of its closure shall become time-barred, in accordance with the Romanian Civil Code, five years after the date on which the Client was notified of the closure by the Bank by registered letter with acknowledgement of receipt.

**2.39.9.** Where the Client's accounts have been closed because they were subject to attachment orders, the Bank may refuse to open new accounts for the Client for a period of up to three months from the closure of the attached accounts.

**2.39.10.** Upon termination of the Contract, the Bank shall provide the Client, free of charge, with a document confirming that all of the Client's obligations arising under that Contract have been discharged.

#### **2.40. Other Rights and Obligations Relating to Payment Accounts and Payment Services**

**2.40.1.** Where applicable, the Bank shall pay interest on the funds held in the accounts, in accordance with the Bank's regulations. The applicable interest rate is specified in the account opening documentation or in the Bank's Schedule of Interest Rates. The Bank may amend the applicable interest rate from time to time. Any new interest rate shall be communicated to Clients by publication at the Bank's branches and on its website. The provisions of Article 1.5.4 shall apply accordingly.

#### **2.40.2. The Client shall be entitled:**

- a) to fund the account by making cash deposits at the Bank's branches or by receiving credit transfers from other accounts held with the Bank or with other banks. For deposits in foreign

currency, the Client shall comply with the foreign exchange regulations in force;

- b) to carry out transactions on the account in accordance with the Contract and the applicable legislation;
- c) to receive, upon request, at any time during the term of the Contract, in paper form or on another durable medium: • a copy of the Contract, • the Fee Information Document, • the Glossary containing the most representative services related to a payment account and their definitions and • the Statement of Fees covering the preceding 12 months;
- d) to receive, where applicable, electronic messages from the Bank regarding currency conversion charges and the exchange rate applicable to card transactions carried out in an EU currency other than the currency of the account linked to the card. The Bank shall send such messages through any of the communication channels agreed under the Contract. The Client shall be entitled to opt out of receiving such messages;
- e) to carry out transactions on the account using the Bank's standard forms, duly completed and reflecting genuine transactions. The Client shall be responsible for the lawfulness of the transactions carried out through the account.

**2.40.3. The client undertakes:**

- a) to carry out transactions on the current account and the revolving account;
- b) to carry out transactions only within the available balance of the account, taking into account, including, the fees due for account administration and for the transactions carried out;
- c) if there is an unauthorised overdraft, to fund the account in order to fully cover the overdraft and the related fees and interest arising from the transactions carried out;
- d) to make at least one monthly payment into the revolving account linked to the credit card, covering at least the amount specified in the credit card agreement;
- e) to review the account status on a monthly basis, using any means made available by the Bank, including the account statement;
- f) to immediately notify the Bank of any lost, stolen, destroyed or cancelled payment instrument, so that the Bank may prevent its further use;
- g) Where an amount is credited to a Client's account by mistake or as a result of a fraudulently executed transaction, the Client shall immediately notify the Bank. The Client shall not be entitled to withdraw, transfer, dispose of or otherwise use that amount, in whole or in part.

**2.40.4. The bank may block:**

- the Client's current account and the use of the card, if (i) the overdraft has not been replenished for three consecutive months, or (ii) there is an unauthorised overdraft. The account shall be unblocked once the reason for blocking ceases to exist, and the card may be used from the day following the unblocking of the account;
- the revolving account linked to the credit card, if the Client fails to fund the account with the minimum mandatory payment amount specified in the credit card agreement.

**2.40.5.** The Bank shall carry out the banking transactions requested by the Client or the authorised signatory on the account only within the available balance of the account, in compliance with its internal rules and with domestic and international banking practices. The Bank shall not use its own funds for these transactions and shall not be liable if such transactions are not carried out due to insufficient funds available in the Client's account.

**2.40.6.** The Bank shall debit the account with the value of transactions carried out in a currency other than the account currency, using the Bank's exchange rate applicable on the transaction date, as communicated to the Client through the account statement.

**2.40.7.** The Bank shall not send unsolicited payment instruments to the Client, except where a payment instrument already provided to the user needs to be replaced.

**2.41. Deposit Guarantee**

**2.41.1.** In Romania, deposits held with Romanian banks are guaranteed by deposit guarantee schemes approved by the National Bank of Romania (NBR). Currently, pursuant to Law No. 311/2015, the only officially recognised deposit guarantee scheme in Romania is the Bank Deposit Guarantee Fund (FGDB).

The Bank participates in the FGDB. Depositors' liabilities towards the Bank shall be taken into account when calculating the compensation payable under the deposit guarantee legislation.

**2.41.2.** For the purposes of deposit guarantee, a deposit means not only the funds available in a deposit account, but also any credit balance (including interest due) which the Bank is required to repay to the Client under the applicable law or agreement, regardless of whether such balance originates from funds held in an account or from temporary situations arising from ordinary banking transactions. By way of exception, certain credit balances referred to in Article 3(5) of Law No. 311/2015 shall not be considered deposits.

**2.41.3. Deposits excluded from guarantee**

No compensation is paid for the following categories of deposits:

- a) Deposits of a credit institution made on own name and account, in compliance with the provisions of Article 64 2 of Law No. 311/2015;
- b) Instruments that fall within the definition of own funds, according to art. 4 (1) (118) of Regulation (EU) No. 575/2013
- c) Deposits resulting from transactions in respect of which final court decisions have been issued convicting the persons concerned of the offence of money laundering. The FGDB classifies deposits under this category based on information received from the competent authorities, from the credit institution whose deposits have become unavailable or from the liquidator appointed by the court, as applicable;
- d) Deposits of financial institutions, according to art. 4 (1) § 26 of the Regulation (EU) No. 575/2013;
- e) Deposits of investment firms, according to art. 4 (1) § 2 of the Regulation (EU) No. 575/2013;
- f) Deposits for which the identity of the holder has not been verified before the deposits become unavailable, in accordance with the legislation on the prevention and combating of money laundering;
- g) Deposits of insurers and reinsurers undertakings, according to art. 2 (A) points 5 and 39 of Law No. 32/2000 on insurance activity and insurance supervision;
- h) Deposits of collective investment undertakings, in accordance with capital market legislation;
- i) Deposits of pension funds;
- j) Deposits of central, local and regional public authorities;
- k) Debt securities issued by the credit institution and liabilities arising out of own acceptances and promissory notes.

**2.41.4.** Additional information regarding deposit guarantee is available on the FGDB website (<http://www.fgdb.ro/>).

**3. SPECIAL PROVISIONS APPLICABLE TO TYPES OF PRODUCTS AND SERVICES**

**3.1. CURRENT ACCOUNT**

**3.1.1.** The current account (or payment account), including the current account with basic features, is an account opened in the name of the Client. It is opened for an indefinite period in the name of a single Client.

The Client holding the account must be at least 18 years of age. By way of exception, a minor Client aged at least 6 may be the holder of a current account underlying a package of products and services intended for minors.

**3.1.2.** The Client shall be required to maintain the current account for as long as any products linked to it remain in place (term deposits, loans, cards, remote-access payment instruments, etc.).

### **3.2. REVOLVING ACCOUNT**

The revolving account (with a credit card linked to it) is an account automatically opened in the name of a single Client following the Client's request for the issuance of a credit card. It can only be used with a credit card linked to it. The revolving account reflects only transactions carried out using the credit card, as well as the related fees, interest, costs and insurance premium.

The revolving account may be funded by any means, including cash deposits or credit transfers from a payment account opened with BRD or another financial institution.

The revolving account may only be debited using the credit card, except in the cases expressly provided for in the credit card agreement.

### **3.3. SAVINGS PRODUCTS**

The Bank currently offers the following savings products:

- term deposits;
- savings accounts;
- the savings service for card payments at POS terminals.

#### **3.3.1. TERM DEPOSITS**

**3.3.1.1.** The deposit account is opened for a fixed term in the name of a single Client and is intended for savings purposes.

The deposit is opened by debiting the current account linked to the deposit, as specified by the Client.

The deposit is closed by crediting the same account.

The current account linked to the deposit must remain open until the deposit matures.

**3.3.1.2. Automatic renewal.** Term deposits may be opened (at the Client's option):

- a) with automatic renewal upon maturity. In this case, upon maturity, a new deposit is automatically opened under the same terms and conditions and at the interest rate applicable at the time of renewal (except for the deposit with a progressive interest rate); or
- b) without automatic renewal upon maturity. In this case, upon maturity, the deposit is closed by crediting the account from which it was opened.

#### **3.3.1.3. Interest**

The Bank pays credit interest on the funds held in the deposit account, payable monthly or upon maturity, at the Client's option.

**Capitalization.** For deposits: (i) without capitalisation, the interest is transferred to the current account linked to the deposit; (ii) with capitalisation, the interest accrues in the deposit account and itself earns interest.

The credit **interest rates** are specified in the deposit opening documentation or in the list of interest rates published by the Bank. They may be adjusted periodically by the Bank in accordance with Article 2.40.1.

**Interest rate type.** The bank offers term deposits with:

- fixed interest rate (standard or negotiated). In their case, the interest rate applicable when the deposit is opened remains unchanged until the contractual maturity date;
- progressive interest.

**Interest calculation.** Interest is calculated based on a calendar year of: (i) 365 days for deposits with a fixed or progressive interest rate; (ii) 360 days for deposits with a negotiated interest rate. By way of exception, for deposits denominated in GBP (pound sterling) and PLN (Polish zloty), interest is calculated based on a 365-day year.

**Taxation.** Interest income from term deposits is taxed in accordance with the tax legislation in force.

**3.3.1.4.** No payments, partial withdrawals, incoming intra-bank or interbank transfers, or subsequent cash deposits are permitted on the deposit account.

If any amount is withdrawn from the deposit before maturity, the deposit is terminated and interest is paid at the demand deposit interest rate applied by the Bank at the time of termination. This interest and the deposit amount are credited to the current account.

For term deposits with a fixed interest rate paid monthly into the current account, upon early termination the Bank deducts from the deposit amount the difference between (i) the interest paid monthly into the current account up to the date of termination of the deposit and (ii) the demand deposit interest applicable to the amounts held in the deposit.

For term deposits with a progressive interest rate, upon early termination, the Bank pays: (i) demand deposit interest if the account is closed within the first 180 days from the opening date; (ii) interest calculated for each completed 180-day period, plus demand deposit interest calculated pro rata for the current period, if the account is closed after the first 180 days from the opening date.

**3.3.1.5.** If the Client requests that the deposit be opened on a non-banking day or public holiday, the deposit shall be deemed to have been opened on the next banking day. If the deposit matures on a non-banking day or public holiday, its maturity date shall be deemed to be that same day.

#### **3.3.2 SAVINGS ACCOUNTS**

**3.3.2.1.** Savings accounts combine the benefits of a current account with those of a term deposit. They are opened for an indefinite period.

**3.3.2.2.** A **minimum balance** is required to open certain savings accounts. This amount is specified in the account opening documentation and must be deposited into the account on the account opening date. Otherwise, the Bank may refuse to open the account. If the Client has other obligations due to the Bank, these shall first be settled from the funds available in the account. Then, if the required minimum balance remains available, the savings account is opened.

Savings accounts may also be subject to a **maximum account balance**, as specified in the account opening documentation. Interest is not included in the calculation of the maximum balance.

**3.3.2.3. The operations allowed** in the savings account are:

- a) cash deposits and withdrawals at the Bank's branches;
- b) cash deposits made by authenticating with the card at MBA terminals supporting this functionality;
- c) incoming intra-bank and interbank transfers;
- d) payments by credit transfer to a current account held by the Client with the Bank.

**3.3.2.4.** Cards cannot be linked to the savings accounts currently offered by the Bank.

**3.3.2.5.** The Bank pays **interest** on the funds held in savings accounts, at a rate determined in accordance with the Bank's regulations. The interest rate is specified in the account opening documentation or in the list of interest rates published by the Bank. The interest rate may be adjusted periodically by the Bank in accordance with Article 2.40.1 and, where applicable, Articles 3.3.2.6, 3.3.2.7 or 3.3.2.8. The new interest rate is communicated to Clients at the Bank's branches and on its website.

The Client agrees that any change to the interest rate may be applied immediately, without prior notice, if the change: (i) is based on the reference interest rate or (ii) is in the Client's favour. The Client is informed of these changes as soon as possible by means of notices displayed at the Bank's branches and on its website.

**3.3.2.6.** For savings accounts opened on or after 16 June 2025, the Bank may change the interest rate in accordance with Article 2.40.1. Interest is calculated on the daily account balance and is capitalised monthly, on the 1st day of each month, regardless of the account opening date.

**3.3.2.7.** For the following savings accounts, which have been withdrawn from the Bank's current offering, the Bank may change the interest rate on the 1st day of each calendar quarter, in accordance with Article 2.40.1:

- **Atustart** accounts (for minors aged 0 to 18) and **Atucont** accounts (for Clients aged 18 or over) – both withdrawn from sale on 16 June 2025;
- **Atusprint** accounts (for minors aged 14 to 18, withdrawn from sale on 26 April 2021);
- **Atustart** accounts (for minors aged 0 to 14, withdrawn from sale on 26 April 2021).

For these accounts, the reference dates for interest calculation are the 1st and 15th of each month, and the balance on which interest is calculated is determined according to the following rules:

**a) Cash deposits and incoming payments** are added to the reference balance for interest calculation as follows:

- those made on the 1st or 15th: from those respective dates;
- those made on any other day of the month: from the next calendar date falling on the 1st or 15th.

Thus, the interest rate is calculated twice a month, on fixed dates: 01 and 15 of the month. For amounts deposited/received on either of these two dates, interest is calculated from the time of the respective deposit/receipt. For amounts deposited or received on any other day of the month, interest is calculated from the next date falling on the 1st or 15th of the month;

**b) Cash withdrawals and credit transfer transactions** reduce the reference balance for interest calculation as follows:

- those made on the 1st or 15th: from those respective dates;
- those made on any other day of the month: retroactively, from the 1st or 15th preceding the transaction.

Thus, for amounts withdrawn/transferred from the account on the 1st or 15th of the month, the reference balance for interest calculation is reduced from those respective dates. Amounts withdrawn/transferred on any other day of the month are taken into account for interest calculation only up to the 1st or 15th preceding the withdrawal.

**3.3.2.8.** For **Smart Cont** accounts (withdrawn from sale on 1 September 2015), interest is calculated on the daily account balance and is capitalised monthly on a fixed date (the 1st of each month), regardless of the account opening date. The Bank may change the interest rate quarterly (on the 1st day of each calendar quarter), in accordance with Article 2.40.1.

**3.3.2.9.** The Client is required to maintain the mandatory **minimum or maximum balance** of the savings account, as stipulated in the contract. The Bank has the right to refuse:

- payment instrument transactions, cash withdrawal transactions and credit transfers, if they would cause the balance to fall below the minimum balance;
- cash deposits and incoming payments, if they would cause the maximum balance to be exceeded. If an incoming credit transfer would cause the maximum balance to be exceeded, the transaction is not processed, and the Bank notifies the Client within 2 business days.

**3.3.2.10.** In the case of a savings account held by a **minor**, after the account holder reaches the **maximum age** applicable to that product:

- The savings account remains open, with no age limit.
- It retains the same identifier (IBAN) and the same contractual terms and conditions. By way of exception, from the date on which the account holder turns 18, the interest rate is replaced by the rate applicable to savings accounts for adult Clients in effect at that time.
- The rights granted by the account holder to authorised persons in respect of the savings account remain in force until: (i) the account holder notifies the Bank in writing of the revocation of the authorisation (by signing the relevant documentation at any BRD branch); or (ii) the authorisation terminates by operation of law, pursuant to applicable law or a decision of the competent court/authority.

**3.3.2.11.** Interest income earned on savings accounts is subject to **tax** in accordance with the tax legislation in force.

### **3.3.3. SAVINGS SERVICE FOR CARD PAYMENTS AT POS TERMINALS**

**3.3.3.1.** Through this service, the Cardholder or User of a debit card may, whenever making a card payment at a POS terminal, automatically transfer an amount from the current account linked to the card to a savings account or a Practicont current account selected by the holder of the account linked to the card.

**3.3.3.2.** The Client may choose one of the following savings methods:

- rounding up the amount spent at the POS terminal to the next amount without decimals (whole amount). The difference between the amount paid at the POS terminal and the whole amount is transferred to the savings account/Practicont current account;
- rounding up the amount spent at the POS terminal to the next multiple of 10. The difference between the amount paid at the POS terminal and the next multiple of 10 is transferred to the savings account/Practicont current account;
- transferring a percentage of the amount spent at the POS terminal. The Cardholder/User may choose one of the predefined values;
- transfer of a fixed amount, regardless of the amount spent at the POS. The Cardholder/User may choose one of the predefined values.

**3.3.3.3.** The holder of the account into which the savings are transferred may be different from the holder of the current account linked to the card enrolled in this service. The two accounts may also be denominated in different currencies.

**3.3.3.4.** The transfers referred to in Article 3.3.3.2 shall be carried out at the end of the day. They are not performed if:

- There are insufficient funds available in the account. In this case, the service is not closed, but transfers that could not be executed are not processed retrospectively;
- the current account attached to the card, the savings account or the Practicont current account was closed;
- the maximum savings account limit has been reached, if any. The Bank notifies Customers in this situation;
- the POS card transaction is cancelled on the day it is made.

**3.3.3.5.** If, after the transfer has been made in accordance with Article 3.3.3.2, the transaction is subsequently cancelled by the Client or the merchant, the amount saved is not affected. Only the actual transaction amount is refunded to the current account.

**3.3.3.6.** For transfers between accounts denominated in different currencies, the applicable exchange rate is BRD's exchange rate for card transactions.

**3.3.3.6.** Loan instalments and other outstanding/due debts are debited as a matter of priority. The amounts to be transferred in accordance with Article 3.3.3.2 are debited last.

**3.3.3.7.** The **modification** of the service takes effect on the day following the signing of the specific form provided by the Bank. The following may be modified, for example: the current account, the debit card, the account into which the savings are transferred, and the savings method.

**3.3.3.8.** The Cardholder/User may request **termination** of the service at any time. It takes effect on the day following the signing of the specific form provided by the Bank.

## **3.4. BANK CARD**

### **3.4.1. Provision (issuance) and delivery of the card and PIN. Card and token activation**

**3.4.1.1.** The Bank offers its Clients debit cards and credit cards.

Debit cards are attached to current accounts in lei and/or foreign currency. They may have, where appropriate, an authorised overdraft facility attached to the account.

The cards can be used in Romania and abroad. Depending on the type of card, the card issuance request may be submitted at the Bank's branches, online (at [www.brd.ro](http://www.brd.ro)), through the YOU BRD service or through the MyBRD Contact service.

#### 3.4.1.2. The account holder can request a card:

- in their own name. In which case, they shall have the status of Cardholder;
- in the name of the Account Proxy on the account linked to the card (who will have the status of Card User), subject to the following conditions:
  - a) the account holder must be the Holder of a card attached to that account;
  - b) for the account proxy, only the same type of card as the Account holder can be requested;
  - c) The Client who is the Account Holder completes the Bank's standard forms for designating a Card User and provides the Bank with the Card User's identification details; and
  - d) The fees associated with the Account Proxy's card and the amounts of the card transactions carried out by the Account Proxy are debited from the Account Holder Client's account.

#### 3.4.1.3. The card is the property of the Bank. The bank may request its return and may authorise a third party to retain it.

The Bank may, in accordance with the law, use authorised subcontractors acting as intermediaries within the card payment system for the production and distribution of cards and account statements, and for verifying the authenticity of the card and the identity of the Cardholder/Card User.

#### 3.4.1.4. Hand-over (delivery) of the card. The Bank delivers the card to the Holder/User within a maximum of 90 calendar days from:

- the date on which the Client requests its issuance, • the date of its replacement or, as applicable, • the date of its renewal.

The card is sent to the Holder/User by courier to the card delivery address specified by them. Only in exceptional, objectively justified cases may the Holder/User request that the card be delivered to one of the Bank's branches.

For card delivery, the Client pays a delivery fee, as specified in the Fee Guide.

The Holder/User may request a change to the card delivery address through:

- a request submitted at one of the Bank's branches, • the MyBRD Contact Service, or • the YOU BRD Service (mobile banking channel).

If the Cardholder/Card User requests the change more than 60 calendar days before the card's expiry date, the Bank delivers the card to the new address; otherwise, the card is delivered to the original address or to a Bank branch (if the Client has not provided a delivery address).

If the card cannot be delivered by courier for reasons beyond the Bank's control, the card is redirected to a Bank branch. The Holder/User is notified by SMS or by telephone that they must collect the card from the branch.

When the card is delivered to a Bank branch or redirected to a branch for delivery, the Client must collect it within a maximum of 90 calendar days from the date of the notification received from the Bank.

#### 3.4.1.5. The PIN code is made available only to the Holder/User, as follows:

- through the You BRD service (mobile banking channel);
- by SMS, to the valid mobile phone number previously declared to the Bank;
- in exceptional cases, on paper, in the BRD branch where the Client completed the card issuance application;
- for cards requested online: always via SMS.

To receive the PIN via SMS, the Holder/User must send, after receiving the card, the unique password via SMS to the phone number indicated in the card's accompanying letter and on the website [www.brd.ro](http://www.brd.ro). **The unique password** consists of:

- the last 4 digits of the card number and the last 4 digits of the CNP (personal identification number).
- for non-resident customers without CNP: the last 4 digits of the card number and the last 4 characters of the identity document declared at BRD.

- for Clients whose CNP has more than 13 characters: the last 4 digits of the card number and the last 4 digits of the first 13 characters of the CNP.

The unique password is written without spaces or symbols. If the CNP contains alphabetic characters, they will be written in lowercase in the unique password.

The PIN request SMS is charged according to the tariff applicable to the Holder/User in relation to his/her telephone operator.

**PIN regeneration.** The PIN via SMS must be requested within a maximum of 90 days from the date of card issuance. After this period has expired, the Client may request PIN regeneration (issuance of a new PIN) by calling MyBRD Contact or at one of the Bank's branches. To regenerate the PIN, the Client pays the fee provided in the Fee Guide. Subsequently, the Customer is notified via SMS that the regenerated PIN is available and receives the necessary instructions to obtain it. The customer must follow these instructions within a maximum of 90 days.

The regenerated PIN is sent via SMS to the Holder/User, no later than 24 hours after completing the request. To activate the new PIN, the first operation with the card must be performed by inserting the card into an ATM terminal. **PIN display.** Through the YOU BRD Service (mobile banking channel), the Cardholder/User can request the display of the existing PIN in the application. If he has difficulties receiving and activating the PIN, he can call the MyBRD Contact service at any time.

#### 3.4.1.6. Card and token activation

##### Card activation

For security reasons, the card is issued inactive to the Cardholder/User. It is automatically activated upon the first transaction authenticated using the PIN, anytime during the card's validity period.

##### Token activation

The Token is activated when the card is enrolled in a digital wallet service on merchants' websites/in their applications or when it is enrolled in Click to Pay.

In case of enrolling the card in Apple Pay/Google Pay:

- if enrolment takes place through the YOU BRD service (mobile banking channel), the token can be activated before the Cardholder/User receives the physical card. In this case, transactions can be made with the token even without the physical card.
- if additional verifications are required, the Cardholder/User must call the MyBRD Contact service to complete the enrolment process.

**Closing the token.** The token associated with the card is closed:

- for the card blocked and restored due to loss/theft/damage/change of Client name: upon restoration of the card;
- for the card renewed upon expiration: upon activation of the renewed card.

In case of token closure:

- to continue using the Apple Pay/Google Pay/Click to Pay service, the Client must enrol the new, restored/renewed card.
- if there were recurring payments for active subscriptions on the old card, the subscriptions must be updated with the new card.
- The Cardholder/User understands that blocking the card or its associated Tokens does not automatically terminate subscriptions, recurring payments or merchant-initiated transactions based on previously stored card details. To stop these payments, the Cardholder/User must contact the merchant/service provider and request cancellation of the subscription or deletion/updating of the stored card details.
- Depending on the rules of the international card organisations and merchants' participation in automatic card details update services, the new card details may be automatically updated with merchants that use stored card details for payments.

**3.4.1.7.** The card is linked to and allows transactions to be carried out on a single current account opened with the Bank in the same currency as the card. By exception:

- a) if the Multicurrency option is enabled, the Cardholder may also link to the card other current accounts opened in their name with the Bank, under the conditions set out in Article 3.4.4.8;
- b) Cash deposits by card at some MBA terminals in the Bank's network can also be made to other accounts, under the conditions of article 3.4.3.2. letter e).

### **3.4.2. Security conditions and notifications in case of unauthorised use of the card**

#### **3.4.2.1.** The Owner/User undertakes:

a) to take all necessary measures to keep the card, the Personalised Security Credentials and the phone/device on which digital wallet applications/services are installed in their possession and secure. They are required to prevent their loss, theft, copying, damage or possession by any other person. The phone must be kept secure because the telephone number provided to the Bank is also:

- an identification key for digital wallet services;
- a secure communication method through which they receive passwords from the Bank by SMS (the 3D Secure security code for online transactions, the card activation code, etc.); and
- a secure method for validating transactions, for example: enrolling cards in Apple Pay/Google Pay/Click to Pay or merchants' applications, authorising online payments, etc.;

The Cardholder/User must exercise caution regarding any communications received by telephone, SMS, email, messaging applications, social media or other channels requesting personal data, banking details, card details, Personalised Security Elements, the installation of applications, access to links, or the carrying out/authorisation of transactions.

The Cardholder/User understands that the caller's identity, the displayed telephone number, the email address, the sender's name or the content of the communication may be falsified or imitated. In the event of any suspicion, the Cardholder/Card User must terminate the communication and contact the Bank exclusively through the official channels communicated by the Bank.

b) to notify the Bank immediately, without undue delay, if any of the following situations arise, so that the Bank can block the card/Token:

- the loss, theft, destruction or unauthorised use of the card/phone/device on which the payment application is installed;
- the Client has disclosed or suspects that they have disclosed the card details, its Personalised Security Credentials or the credentials used to access remote banking services to an unauthorised person;
- the Client has been induced to install applications, access links or authorise transactions as a result of an attempted fraud.

The notification must be made through the MyBRD Contact service, using the contact details specified in Section 1.2. Definitions and interpretation.

The card may also be blocked directly by the Client through the YOU BRD service (mobile banking channel). Blocking the card automatically also blocks the Token.

The user can request blocking only for their own cards. The Holder may request blocking for both their own cards and the cards of the Users.

If the Holder/User fails to comply with these obligations, they shall be deemed to have acted with gross negligence and shall bear the financial losses in full.

d) to periodically check the account status and transactions made, at least once a month. If the Client notices any incorrect, unauthorised or fraudulent transactions, they must notify the Bank as soon as possible, in accordance with Section 3.4.5. (Chargebacks).

**3.4.2.2.** The Holder/User has the following obligations regarding the PIN and the e-Commerce Password, failing which they shall bear the resulting loss in full:

- a) upon receipt of the sealed envelope containing the PIN, to memorise the PIN and destroy the envelope; if the PIN was received by SMS, the PIN must be memorised, and the SMS must be deleted;
- b) if the PIN was received on paper in an envelope, to notify the Bank immediately if the envelope was not sealed;
- c) not to write the PIN or the e-Commerce Password on the card or on any other items kept together with the card;
- d) to use the PIN and the e-Commerce Password in such a way that they cannot be seen by other persons;
- e) not to disclose to other persons the card details, its Personalised Security Credentials or the credentials used to access remote banking services. This obligation applies regardless of who makes the request (including Bank staff, the police or other authorities) and regardless of the form in which the request is made (verbally, in writing, by accessing links received by email or through other means of communication).
- f) if the PIN or any other Personalised Security Credentials have become known to another person, to notify the Bank immediately and request that the card and the Tokens be blocked and that a new card be issued (bearing the applicable fee). Otherwise, the Cardholder/User shall bear all losses relating to unauthorised payment transactions where such losses result from fraud or from the intentional or grossly negligent failure to comply with their obligations under the Contract;
- g) to ensure the security of the device from which online transactions are initiated, by complying with the following minimum requirements:
  - the use of antivirus and anti-spyware software, with signatures updated regularly (daily), which scans the device on a regular basis;
  - installing and activating a firewall;
  - keeping the operating system and browsers (Internet Explorer/Firefox/Chrome/Safari/Edge) updated with the latest versions and security patches.

**3.4.2.3.** The above obligations regarding the safekeeping of the PIN and the e-Commerce Password also apply to the other Personalised Security Elements.

**3.4.2.4.** The Bank never requests login credentials, account identification details or Personalised Security Elements. Any such attempt is considered an attempted fraud and must be reported to the Bank immediately.

**3.4.2.5.** In the event of cyberattacks, the Client agrees to cooperate with the Bank in identifying the source of the attack.

**3.4.2.6.** The Cardholder/User may view the PIN through the YOU BRD service. If they no longer remember the PIN and do not have access to YOU BRD, they may request PIN regeneration by calling MyBRD Contact or at one of the Bank's branches. PIN regeneration is charged according to the Fee Guide.

**3.4.2.7.** The Cardholder/User may request the reissue (replacement) of a lost, stolen, damaged, demagnetised, potentially compromised or captured card by calling the MyBRD Contact service. They shall pay the applicable fee in accordance with the Fees Guide.

**3.4.2.8.** The Bank blocks the card and the associated Tokens (at the Client's request) as soon as it is notified of the loss of the card/phone or device on which the digital wallet application is installed, in the manner described above.

The card blocking becomes effective:

- if blocked by the Bank: after the Bank has taken the appropriate measures and the Cardholder/User has received confirmation that the card has been blocked;
- if blocked by the Client through the YOU BRD service (mobile banking channel): as soon as the blocking operation is completed.

**3.4.2.10.** For certain transactions that it considers unusual or suspicious, the Bank may ask the Cardholder/User to confirm that they carried out the transaction. Therefore:

- The Bank sends an SMS to the Cardholder/User requesting them to confirm the transaction by replying to the SMS sent by the Bank.
- If the Cardholder/User confirms the transaction, the card can continue to be used.
- If the Cardholder/User does not confirm the transaction or does not respond to the Bank's SMS within a maximum of 5 minutes of receiving it, the card is blocked. The Bank notifies the Cardholder/User through a new SMS message that the card has been blocked and what steps to follow.
- If the Cardholder/User has not declared any phone number in the Bank's database, or if none of the declared numbers are no longer up to date, the card is blocked for security reasons, until the Client confirms those transactions.

**3.4.2.11.** The Bank notifies the Cardholder/User, via SMS message, if the card is blocked because it is suspected of having been compromised.

### **3.4.3. Using the Card**

**3.4.3.1.** The card can only be used by the Holder/User in whose name it was issued. The card may be used from the date it is received until the last calendar day of the month indicated on the card.

**3.4.3.2.** Holders/Users may carry out the following transactions using the card:

- a) purchasing goods and services from Acceptors displaying the logo of the card organisation specific to the type of card held, including contactless transactions. As an exception, the Sprint card cannot be used to pay utility or service bills at merchants. For online purchases, it is recommended to carry out transactions on secure websites enrolled in the 3D Secure service and displaying the "Verified by Visa" or "Mastercard SecureCode" logos;
- b) payment of obligations to public administration authorities displaying the card acceptance logos (except Sprint card);
- c) cash withdrawals at the counters of banking units of other Merchants, upon presentation of an identity document (if requested);
- d) obtaining cash from ATMs that have the card acceptance logos displayed;
- e) cash deposits at MBA/ROBO terminals within the Bank's network, subject to the following provisions:
  - at ROBO terminals, cash deposits may only be made into the current account linked to the card used.
  - At MBA terminals:
    - (i) cash deposits may also be made into other current accounts linked to the card with the Multicurrency option enabled, as well as into savings accounts or loan repayment accounts for which the Clients are Account Holders or Account Proxies. As an exception, minor Cardholders may make cash deposits only into their own accounts;
    - (ii) if cash is deposited into accounts denominated in a currency other than that of the card, the Bank performs the necessary currency exchange using its own exchange rate for card transactions applicable on that day;
    - (iii) the card usage limits remain unchanged, regardless of the number of accounts into which cash is deposited using the card.
- f) payment of utility bills at ATM/MBA/ROBO terminals within the Bank's network;
- g) operations with Token:
  - contactless payments at merchants, when the card is linked to an Apple/Android device compatible with NFC Technology (smartphone, smartwatch, etc.);

- online transactions on merchants' websites and in their applications that accept card payments;
- online transactions on merchants' websites and in their applications that accept payments via Click to Pay;
- cash withdrawals at terminals compatible with contactless technology (Mastercard cards only);

**h)** Quasi-Cash transactions. These transactions are carried out at merchants (including non-bank financial institutions, foreign exchange offices, etc.) for the purpose of obtaining cash or cash-convertible goods (e.g. casino chips, lottery tickets, bets, etc.), rather than for the purpose of purchasing goods or services. They do not include cash advance transactions;

**i)** money transfer transactions. These transactions are carried out for the purpose of transferring money, using the card, from the current account or the account linked to the credit card to another account. Examples of such transactions include (without limitation) transactions involving funding, by card, an account opened with another financial institution; transactions involving payment by card of instalments on loans granted by other financial institutions, including instalments payable under instalment payment schemes offered by merchants; or funding an electronic wallet or a digital application (for example: PayPal, Wise, TikTok, Facebook, etc.);

**j)** access to other optional services offered by the bank, based on special requests (except Sprint card);

**j)** transfer of funds between own and third-party accounts (except Sprint card);

**l)** obtaining information on the balance of the current account or revolving account at ATMs, using the PIN;

**m)** changing the PIN at the Bank's ATMs.

**3.4.3.3.** For some cards, the Bank may attach additional assistance and insurance services free of charge. These are communicated to the Holder/User.

**3.4.3.4.** Regardless of the currency of the accounts to which the cards are linked, the cards may be used both domestically and abroad, subject to the applicable foreign exchange regulations. Use is limited to the available funds in the current accounts (including any authorised overdraft, where applicable) or in the revolving accounts linked to the cards.

**3.4.3.5. Usage limitations:** For the security of transactions and the protection of the Cardholder/User, the Bank, card organisations or European banking authorities may set limits on the number and value of transactions that may be carried out using the card within a given period.

These limits may be consulted: (i) in the letter accompanying the card or in the annex to the credit card agreement, (ii) at the Bank's branches, (iii) on the Bank's website, (iv) by calling the MyBRD Contact service.

The Cardholder may request a change in usage limitation, both for the card issued in his name and for the User. The request can be made in bank branches, through MyBRD Contact or through the YOU BRD service (mobile banking channel). The Bank will communicate to the Cardholder/User the decision regarding the request received.

**3.4.3.6.** The bank may monitor card transactions for security reasons to prevent their fraudulent use.

**3.4.3.7.** For certain types of cards, the Bank may require collateral to be provided in the form of an amount of money blocked in an account (collateral deposit) opened with BRD.

**3.4.3.8.** The holder (and the legal representative, if applicable) shall be liable to the Bank for all payment obligations arising from the use of the card by any User. These automatically become payment obligations owed to the Bank and must be paid in accordance with the Contract.

**3.4.3.9.** The Bank automatically debits the amounts corresponding to the value of card transactions from the current account/revolving account linked to the card.

In case of lost, stolen or fraudulently used card:

- this debit is made until the Cardholder/User notifies the Bank of the loss/theft/fraud of the card.
- The exception is transactions made at terminals operating in offline mode. In their case, the account is debited automatically, without requiring the Bank's authorisation. Thus, the value of these transactions is debited from the account even after the Bank receives notification of the loss/theft/fraud of the card. If the funds in the account do not cover the value of transactions made at these terminals, the uncovered difference is recorded as an unauthorised overdraft.

**3.4.3.10.** The use of cards for illegal purposes is prohibited, including for the purchase of goods or services prohibited by the laws of the country in which the card is used. If the Bank identifies credit transactions in the Client's account that cannot be justified by the transactions carried out using the respective card, it may block these amounts for a maximum period of 30 days for further investigation.

**3.4.3.11.** The Bank may temporarily suspend the card transaction system for IT system optimisation work or for other technical reasons. During this period, Clients may be unable to carry out certain card transactions. The Bank notifies Clients about these interruptions through the website [www.brd.ro](http://www.brd.ro).

#### **3.4.3.12. Click to Pay functionality**

This functionality allows Cardholders/Card Users to make online payments to merchants without having to manually enter their card details at the time of payment. For payment security purposes, the actual card details stored in Click to Pay are replaced with a secure token. In this way, merchants do not have access to the actual card details.

Click to Pay allows online payments to be made only at merchants that accept this payment method.

The manner in which online card payments are made through Click to Pay is described in detail below in Article 3.4.4.1(d.2).

The Click to Pay functionality is automatically enabled for all debit/credit cards issued by the Bank to individual Cardholders/Card Users who have an email address and mobile phone number registered with the Bank and have activated the YOU BRD service (mobile banking channel). Cards are enrolled in a Click to Pay profile associated with the Cardholder/User, managed by the card organisation.

Cardholder/Users who do not wish to benefit from this functionality can deactivate it at any time, through the YOU BRD Service (mobile banking channel), "Cards" section. They have the possibility to reactivate it later, as well as to temporarily suspend it, if they wish, also through the YOU BRD Service.

The card organisation may decide to suspend or discontinue the Click to Pay functionality. In this case, the Bank will notify the Cardholders/Users as soon as possible. The Bank shall not be liable for any inconvenience or loss suffered by Cardholders/Card Users in such situations, which are beyond the Bank's control.

Further information on the Click to Pay functionality is available in the document setting out the applicable terms and conditions, published on the Bank's website here: [www.brd.ro/click-pay](http://www.brd.ro/click-pay).

In connection with the Click to Pay functionality, the Bank processes a series of personal data of the Cardholders/Users. The document referred to in the preceding paragraph sets out in detail what personal data is processed, how and for what purposes it is processed, as well as the rights of Cardholders/Users in relation to such processing.

#### **3.4.4. Authorisation and Execution of Card Payment Transactions**

**3.4.4.1.** A card payment transaction must be authorised by the Cardholder/User, as follows:

**(a)** By inserting the card into a terminal that reads the chip/magnetic stripe and the card data (including for offline transactions),

followed by signing the receipt and/or entering the PIN at the terminal.

**(b)** If the contactless functionality is used: by holding the card close to the terminal (with or without entering the PIN). Notes:

- For contactless payments that do not exceed a limit set by the international card organisations, entering the PIN is not required;
- After every 5 consecutive contactless transactions made without entering the PIN, the next transaction (the 6th transaction) requires the PIN to be entered;
- If the cumulative amount of consecutive contactless transactions made without entering the PIN exceeds 150 EUR (or the equivalent in RON), the next transaction requires the PIN to be entered.
- The 150 EUR limit does not include • contactless transactions carried out at unattended terminals within the European Economic Area (for the purpose of paying for transport tickets, parking fees, etc.) and • transactions carried out at contactless terminals outside the European Economic Area.
- The Client may request that the contactless functionality be blocked or unblocked by calling MyBRD Contact.

**(c)** For transactions carried out by means of distance communication (e.g. online payments) – by providing the card number, expiry date and Personalised Security Credentials, as follows:

**(c.1)** If the transactions are carried out at Merchants that have implemented the 3D Secure service, the Cardholder/User:

- authenticates through the YOU BRD Service (mobile banking channel), using biometric authentication or by entering the mPIN code to access the application;
- enters the payment details on the payment screen on the Merchant's website;
- receives a notification on their mobile phone (smartphone) to authenticate the transaction through the YOU BRD Service (mobile banking channel);
- may authenticate the transaction within 10 minutes of its initiation.

**(c.2)** By way of exception, if the Cardholder/User does not have a smartphone or does not have the YOU BRD Service, they may use the e-Commerce Password to authorise online payments. Therefore:

- on the payment screen, they select the mobile phone number (if they have provided more than one) on which they will receive the one-time transaction validation code;
- confirmation is completed by entering the 3D Secure code in the designated field on the payment screen;
- if the Cardholder/User has no telephone number registered in the Bank's database, or if none of the telephone numbers displayed is up to date, the transaction cannot be completed. The Cardholder/User may notify the Bank of a new telephone number at any of the Bank's branches.

**(c.3)** The Bank is not liable for unsecured online transactions for which Merchants: • choose not to request the one-time validation code; or • accept the payment even if the Cardholder/User abandons the payment before entering the one-time validation code.

**(c.4)** If the online transactions are carried out at a Merchant within the European Economic Area and:

- have a value of less than 30 EUR, the Client gives consent by providing the card details. After every 5 consecutive transactions carried out in this manner, or once the cumulative value of consecutive transactions carried out in this manner exceeds 100 EUR, Strong Customer Authentication may be deemed necessary.
- have a value greater than 30 EUR, the Client gives consent by providing the card details. If Strong Customer Authentication is deemed necessary, the provisions of the Contract regarding Strong Customer Authentication using biometrics, mPIN or the e-Commerce Password shall apply.

(c.5) Online payments to a Merchant within the European Economic Area may be made without Strong Customer Authentication if they meet the conditions laid down by the applicable European legislation.

(c.6) The Bank may choose not to apply Strong Customer Authentication to low-risk online transactions. The risk level is determined based on the Cardholder/User's transaction profile, taking into account several parameters such as: • payment history with a particular merchant, • transaction value, • repeated transactions with the same merchant, • subscription payments, • payments to a trusted beneficiary, • payments made in applications or on websites that do not use Visa Secure and/or Mastercard Identity Check services, using cards previously saved in those applications/websites, • payments made from the same device, using the same declared Cardholder/User name, telephone number, email address, delivery address, etc.

(d) For **token-based payment transactions**, the Client gives consent by:

(d.1) for contactless payments: by unlocking the mobile device (using • biometrics/mPIN or • in the case of Apple Watch, by quickly pressing the device's side button twice in succession), followed by holding the mobile device on which the token is installed close to the payment terminal;

(d.2) for online payments on merchants' websites and in merchants' applications displaying the Apple Pay/Google Pay/Click to Pay option: by giving consent on the website/in the application to complete the payment via Apple Pay/Google Pay/Click to Pay.

In the case of online payments via Click to Pay:

- for the first payment via Click to Pay made from a particular device (phone, tablet, computer, etc.), the Client is required to verify their identity using a one-time verification code (OTP – One Time Password) sent to the telephone number or email address associated with the Click to Pay service. This code must be entered on the payment screen. It helps validate the device and its subsequent recognition. The Client may then choose not to receive this validation code for each subsequent Click to Pay payment made from the same device;
- the Client is shown a list of their cards enrolled in Click to Pay, based on their email address;
- the Client selects the card they wish to use to make the payment. There is no need to manually enter the card details (card number, CVV, expiry date), as they are pre-filled on the payment screen;
- the Client authorises the payment using the methods described in points c1–c6) above.

(d.3) for cash withdrawals at terminals with contactless functionality that support Apple Pay/Google Pay: by holding the mobile device on which the token is registered close to the terminal and entering the card PIN on the terminal.

**3.4.4.2.** The Cardholder/User must verify that the transaction details (amount, currency, merchant name) are correct before authorising the transaction. They must keep the receipt and any other supporting documents as evidence in case of discrepancies. The Cardholder/User is responsible for the consequences of failing to comply with these obligations.

**3.4.4.3.** The card is blocked if the PIN or CVV2/CVC code is entered incorrectly 3 consecutive times. To unblock the card, the Cardholder/User must either (i) contact the Bank (at any branch or at the telephone number shown on the card) or (ii) unblock the card through the YOU BRD service (mobile banking channel).

**3.4.4.4.** As soon as the Cardholder/User authorises a card transaction, the Bank blocks the corresponding amount for

settlement. This prevents the same amount from being used for another transaction. Transactions for which the Merchant does not request authorisation from the Bank are an exception – these will be debited from the account upon receipt of the settlement report.

The Merchant initiates the settlement of an amount. The Merchant's bank submits the amount for collection by sending the transaction (via Visa/Mastercard) to the card-issuing bank.

The Cardholder/User may check the blocked amounts (i) through the YOU BRD service, in the "Blocked amounts" section, and (ii) at the Bank's ATMs, in the following section: "List of the Last 10 Transactions".

The amount blocked following approval of the transaction cannot under any circumstances be unblocked by the Bank or withheld from settlement, as it constitutes a guarantee to the acquiring bank that it will receive the funds for • the amount dispensed by its ATM or • the services provided or goods sold by the Merchant. By way of exception, the amount blocked following a card transaction may be unblocked by the Bank in the following situations:

- (i) if the Merchant or its bank confirms in advance that the transaction was not completed and will not be submitted for settlement;
- (ii) if the Merchant does not submit the transaction for settlement within the timeframe established by the card organisations (Mastercard/Visa), the Bank automatically unblocks the corresponding amount within a maximum of 10 calendar days from the date it was blocked. However, even after this automatic unblocking, the Merchant may still submit the transaction for settlement. In this case, the Bank debits the account linked to the card by the respective amount. If the full amount is no longer available in the account on the settlement date, the difference between the transaction amount and the available balance in the account is recorded as an unauthorised overdraft.

**3.4.4.5.** The date of a card transaction is the date on which the transaction is recorded at the acquiring bank's Terminal. It takes into account the date and time in the geographical area where the Terminal is located. The Bank is not liable if other Merchants settle the transaction using an incorrect date (a date other than the date on which the transaction was actually carried out) or other incorrect transaction details.

**3.4.4.6.** The Bank debits the amount of card transactions from the current account/revolving account linked to the card upon receipt of the settlement report for those transactions.

**3.4.4.7. Foreign Exchange.** In the case of cards for which the Multicurrency option is not enabled, for transactions involving currency exchange (international transactions or domestic transactions in a currency other than that of the account):

- the card organisation performs the currency exchange (at the exchange rate set by it on the date the transaction is submitted for settlement) between: (i) the currency of the original transaction and (ii) the settlement currency;
- in order to debit the amount of the transaction from the current account/revolving account linked to the card, the Bank performs a currency exchange (using the Bank's exchange rate) between (i) the transaction amount in the settlement currency and (ii) its equivalent in the currency of the current account.

**3.4.4.8. Multicurrency option**

This option allows the Cardholder to link to the card other current accounts opened in their name with the Bank, in addition to the RON current account initially linked to the card, provided that:

- (i) the currency of these accounts must be one of the currencies for which the Multicurrency option is available (as specified on the Bank's website, [www.brd.ro](http://www.brd.ro)); and
- (ii) if the Cardholder holds several current accounts in the same currency opened with the Bank, only one account in that currency may be linked to the card.

The Multicurrency option is available only for RON-denominated debit cards issued in the name of Cardholders aged at least 18. This option is not available for cards issued to authorised Users or for cards with minor Cardholders.

The Multicurrency option is not enabled by default when the card is issued. If the Cardholder wishes to use this option, they must expressly request its activation through the YOU BRD service or at any of the Bank's branches (by completing the relevant forms). Upon activation, the Cardholder specifies • the current accounts they wish to link to the card and • the order in which these accounts will be debited when card transactions are carried out.

Subsequently, the Cardholder may modify these options and disable the Multicurrency option at any of the Bank's branches or through the YOU BRD service.

If the Multicurrency option is enabled, the amount of the card transaction is debited from one of the current accounts linked to the card, in accordance with the debit order established by the Cardholder as described above. By way of exception, the RON current account linked to the card is always debited first. Therefore:

a) For transactions carried out in RON:

- The Bank debits the RON account linked to the card;
- If there are insufficient funds available in the RON account, the Bank debits one of the other accounts linked to the card, in the order established in advance by the Cardholder as described above and performs the necessary currency exchange.

b) For transactions carried out in a foreign currency, where that currency corresponds to an account linked to the card:

- The Bank debits the account denominated in the currency of the transaction;
- If there are insufficient funds available in that account, the Bank debits the RON account and performs the necessary currency exchange;
- If there are insufficient funds available in the RON account, the Bank debits one of the other accounts linked to the card, in the order established in advance by the Cardholder as described above and performs the necessary currency exchange.

c) For transactions carried out in a foreign currency, where the currency differs from the currencies of the accounts linked to the card:

- The Bank debits the RON account and performs the necessary currency exchange;
- If there are insufficient funds available in the RON account, the Bank debits one of the other accounts linked to the card, in the order established in advance by the Cardholder as described above and performs the necessary currency exchange.

The currency exchanges referred to above are performed at the Bank's exchange rate for card transactions, as displayed on the website [www.brd.ro](http://www.brd.ro).

The fees applicable to card transactions are those corresponding to transactions on the current account from which the amount of the card transaction is debited, in accordance with the Fee Guide.

The card usage limits remain unchanged, regardless of how many current accounts are linked to that card.

**3.4.4.9.** The exchange rate applicable on the date the transaction is authorised may differ from the exchange rate applicable on the date the transaction is settled. If, due to this fluctuation, the available balance in the account on the settlement date is no longer sufficient to cover the amount of the transaction, the uncovered difference is recorded as an unauthorised overdraft.

**3.4.4.10.** Details on the exchange rates applicable to card transactions involving currency exchange are available at [www.brd.ro](http://www.brd.ro) and/or on the websites of the international card organisations.

### **3.4.5. Chargebacks**

#### **3.4.5.1. Initiating a chargeback**

If the Cardholder/User identifies an unauthorised or incorrectly executed payment transaction in their account, they have the right to initiate a chargeback.

To do so, the Cardholder/User must complete the specific form made available by the Bank at its branches or call the MyBRD Contact service.

The chargeback must be initiated without undue delay, but no later than 13 (thirteen) months from the date of the debit. The Bank provides Clients with internet and mobile banking services, MyBRD SMS and balance enquiry at BRD terminals (ATM/ROBO), enabling them to immediately identify transactions carried out and notify the Bank as soon as possible (no later than 2 months from the date the transaction is recorded in the account) of any unauthorised or incorrectly executed payment. If the Bank is not notified within this period, the transaction shall be deemed accepted.

**3.4.5.2. Information and supporting documents.** The Cardholder/User is required to provide the Bank with all information and documents supporting the chargeback within a maximum of 10 calendar days of the request. Without such information and documents, the Bank cannot resolve the dispute.

**3.4.5.3. Response deadline.** The Bank handles chargebacks in accordance with the rules of the card schemes and applicable law. The Bank's response shall be communicated to the Cardholder/User within a maximum of 35 business days from receipt of the written notification.

**3.4.5.4. Refund.** The Bank shall refund the Client the amount of the unauthorised payment transaction no later than by the end of the following business day after becoming aware of or being notified of the transaction, unless it has reasonable grounds to suspect that fraud has been committed and communicates those grounds in writing to the competent national authority.

**3.4.5.5. Reporting to the criminal investigation authorities.** In addition to notifying the Bank in accordance with Article 3.4.2.1(b) above, the Cardholder/User is also required to report the matter to the criminal investigation authorities in the following cases:

- within no more than 24 hours of the occurrence of the event, in the event of theft or loss of the card, telephone or device on which the digital wallet service is installed, or fraudulent use of the Personalised Security Credentials (circumstances that resulted in unauthorised transactions); and/or
- when expressly requested by the Bank to do so, within 10 days from the date of the request.

In these cases, the chargeback shall be accompanied by the Cardholder/User's declaration that they have reported the matter to the criminal investigation authorities and by supporting evidence thereof.

**3.4.5.6. Card blocking.** If the Cardholder/User disputes a transaction on the grounds that they do not recognise it, did not authorise it or suspect it may be fraudulent, in order to prevent further transactions of the same type, they are required to block the card through the YOU BRD service (mobile banking channel) or request that the Bank block the card by contacting the MyBRD Contact service.

If the Cardholder/User does not block the card using one of the methods indicated above or informs the Bank that they do not wish the card to be blocked as described above, any chargebacks initiated in respect of transactions subsequent to the transaction already disputed may not be resolved in their favour.

Furthermore, in such situations, the Bank has the right to block the card on its own initiative.

**3.4.5.7. Contacting the Merchant.** If the User/Cardholder has any suspicions regarding transactions carried out online and/or using a card enrolled in payment applications (e.g. PayPal, Google, Apple, iTunes, Uber, etc.) or via Click to Pay, before initiating a chargeback, the Cardholder/User must contact the Merchant

directly for details regarding the transactions concerned and provide the Bank with supporting evidence thereof.

**3.4.5.8.** In the case of recurring subscription transactions, the Cardholder/User shall request that the merchant cancel the subscription in accordance with the terms agreed with the merchant. If the merchant continues to charge amounts after the subscription has been cancelled, the Cardholder/User may initiate a chargeback, accompanied by proof of cancellation.

**3.4.5.9. Contacting the insurer.** If a service provider (e.g. a travel agency, airline, etc.) becomes insolvent and no longer provides the services paid for by the Cardholder/User using the card, the Cardholder/User shall first contact the insurer specified in the insolvency notice or communicated by the service provider in order to obtain a refund. If the Cardholder/User does not receive a response from the insurer within 60 days, the Cardholder/User may initiate a chargeback with the Bank, accompanied by proof of the claim submitted to the insurer.

**3.4.5.10.** The Cardholder/User is directly liable for transactions carried out under **agreements concluded with merchants (by accepting the applicable terms and conditions)**. The Bank shall not be liable for any direct or indirect losses suffered by the Cardholder/User in connection with such contracts (e.g. financial losses resulting from financial advisory services, loss of anticipated profits, reputational or image damage, etc.).

**3.4.5.11.** An online order for the purchase of goods or services may only be cancelled by the Cardholder/User who initiated it, in accordance with the terms and conditions agreed at the time of the transaction. The bank cannot intervene in this process. To cancel the order, the Cardholder/User must contact the merchant. If the goods have been received but do not correspond to those ordered, before initiating a chargeback with the Bank, the Cardholder/User must return the product(s) received to the Merchant in accordance with the Merchant's cancellation policy and provide the Bank with proof of return. If the Cardholder/User has requested and obtained cancellation of the order from the merchant, or has returned the product, but the merchant nevertheless fails to refund the amount, the Cardholder/User may initiate a chargeback (attaching proof of the merchant's confirmation of the order cancellation or proof of return of the products).

**3.4.5.12.** If the chargeback proves to be unjustified and the amount of the disputed transaction has already been refunded by the Bank to the Cardholder/User's Account, the Bank shall debit the Account with the amount of the respective transaction and charge the unjustified chargeback fee in accordance with the Fee Guide.

#### **3.4.6. Card blocking**

**3.4.6.1.** Blocking the card is the operation whereby the Bank prevents the use of a card without closing the current/revolving account linked to the card.

**3.4.6.2.** The Bank has the right to block the card in the following situations (without prior notice, unless otherwise provided below):

- a) no transactions have been recorded in the current account linked to the card for 6 months and its balance is less than 15 EUR. In this case, the Bank shall notify the Cardholder/User in writing at least 2 months before the card is blocked;
- b) the new or renewed card is not collected from the Bank's branch within the specified period;
- c) for reasons related to the security of the payment instrument;
- d) there is a suspicion of unauthorised or fraudulent use of the card;
- e) the card has an attached credit line and there is an increased risk that the Cardholder may be unable to meet their payment obligations;
- f) the card is used repeatedly for transactions that exceed the available balance of the account;
- g) the card is used improperly;
- h) at the request of the competent authorities;
- i) the available account balance is exceeded. In this case, the Bank may also charge penalty interest;

j) the information provided by the Cardholder/User to the Bank proves to be incorrect, incomplete or false;

k) in the situations provided for in specific contracts (for example, for cards enrolled in digital wallet applications/services).

In the cases referred to in points c), d) and e) above, the Bank notifies the Cardholder of the blocking and the reasons for it by any available means (telephone, fax, email, letter, etc.). Where possible, the Cardholder/User shall be notified before the card is blocked and, at the latest, immediately after it is blocked. By way of exception, no notification shall be sent if there are objectively justified security reasons or if notification is prohibited by law.

**3.4.6.3.** The Bank shall unblock the card or replace it with a new card (subject to a fee in accordance with the Fee Guide) once the reasons for blocking no longer exist.

**3.4.6.4.** Blocking the Cardholder's card may also result in the Users' cards being blocked.

**3.4.6.5.** When it deems necessary, the Bank may:

- a) refuse to authorise a card transaction;
- b) cancel or block the use of the card;
- c) replace the card, for security reasons; and
- d) refuse to provide a new card or replace the card.

The Bank notifies the Cardholder/User about these measures as soon as possible. The Cardholder/User remains responsible for the transactions performed with the card.

#### **3.4.7. Liability of the Parties for Card Transactions**

**3.4.7.1.** The Cardholder/User (and their legal representative, if applicable) shall be liable for transactions carried out up to the time the Bank is notified of the loss, theft or unauthorised use of the card or the Personalised Security Elements. In such cases, the Cardholder/User shall bear financial losses up to a maximum amount of 30 EUR (or the equivalent in RON).

**3.4.7.2.** By way of exception, the Cardholder/User shall bear the losses in full (i.e. the limit set out in the preceding paragraph shall not apply) if:

- acted negligently, in bad faith or with fraudulent intent;
- used the card in breach of the Contract; or
- did not notify the Bank, without undue delay, of the loss, theft or unauthorised use of the card.

**3.4.7.3.** The Cardholder/User shall not bear any losses resulting from the use of a lost or stolen card or from the unauthorised use of the card in the following situations:

- a) if the loss, theft or unauthorised use could not have been detected by the Cardholder/User before the payment was made;
- b) if the loss of the card was caused by an act or omission of the Bank;
- c) after notifying the Bank in accordance with the Contract (unless the Cardholder/User has acted fraudulently);
- d) if the Bank failed to apply Strong Customer Authentication when it was required to do so.

**3.4.7.4.** The Cardholder/User is required to indemnify the Bank for any debits, losses or expenses resulting from the Cardholder/User's failure to comply with the Contract. The Cardholder/User is also required to indemnify the Bank where they are found to be liable for transactions that were unjustifiably disputed.

**3.4.7.5.** The Bank is not liable for losses caused by the unauthorised use of a card (lost/stolen/used without authorisation) if • the Cardholder/User acted fraudulently or • intentionally, through fault or gross negligence, failed to comply with their obligations to keep the Personalised Security Credentials safe.

**3.4.7.6.** The Bank shall not be liable for:

- a) damages caused by exceeding the available account balance or the card usage limit;
- b) the manner in which the card is accepted by merchants, the refusal to accept the card by a merchant/third party or if a request to authorise a card transaction is refused, regardless of the reason;

c) delayed or erroneous debiting of card transactions, caused by third parties (e.g. delayed transmission of transactions for settlement).

#### **3.4.8. Validity of the card. Automatic renewal. Termination of the Card Contract**

**3.4.8.1.** The Card Agreement shall be valid from the date it is entered into until the card's expiry date, with the possibility of automatic renewal.

**3.4.8.2.** The Bank shall notify the Cardholder/User in writing of the card's expiry and, where applicable, the automatic renewal of the Contract.

**3.4.8.3.** Upon expiry of a card, the Contract relating to the card is automatically renewed and the Bank provides the Cardholder/User with a new card if the conditions established for card renewal are met and the Cardholder/User does not notify the Bank that they wish to give up the card (terminate the Contract), as set out below.

**3.4.8.4.** The card shall not be renewed if the Cardholder/User notifies the Bank of their intention to discontinue the card at least 2 months before its expiry date.

**3.4.8.5.** The cards shall be automatically renewed upon expiry only if all of the following conditions are met:

- a) The card is not blocked because of the application of the provisions of the Contract or non-compliance with the contractual terms;
- b) The current account/revolving account is not blocked because of account enforcement (freezing) proceedings;
- c) The current account/revolving account does not have an unauthorised overdraft;
- d) The Cardholder/User meets the Bank's risk criteria;
- e) The Cardholder/User has not notified the Bank of the unilateral termination of the Contract in accordance with the procedure set out above;
- f) transactions have been recorded in the current account/revolving account during the last 6/12 months (depending on the type of card) and the minimum available balance required by the Bank is maintained;
- g) The Cardholder maintains the status required for the relevant type of card, where applicable, in accordance with the card-specific documentation);
- h) The Cardholder meets the age requirements applicable to the card (e.g. in the case of cards for minors and credit cards).

**3.4.8.6.** If a type of card is withdrawn from the Bank's product offering, it may be replaced upon renewal with another similar type of card. In this case, the Bank shall inform the Cardholder/User in advance.

**3.4.8.7.** The Card Agreement shall terminate automatically if the Cardholder/User fails to collect the new, replacement or renewed card within the period specified in the Agreement.

**3.4.8.8.** Upon termination of the Card Agreement for any reason, the Bank shall have the right to block the balance of the current account linked to the card or the available limit in the revolving account for 30 calendar days following termination. This blocking is carried out to allow transactions made with the card prior to termination and submitted for settlement by Merchants during this period to be settled. The Agreement shall remain in force until all such transactions have been settled.

### **3.5. REMOTE BANKING SERVICES**

#### **3.5.1. General Principles**

**3.5.1.1.** The Client may subscribe to certain services and carry out certain transactions through remote banking services, in compliance with the Agreement and applicable legislation.

The provisions of subsection 3.5.1. "General Principles" apply:

- both to the remote banking services governed by Section 3.5 – REMOTE BANKING SERVICES;

- and to remote banking services governed by separate agreements entered into between the Client and the Bank (e.g.: YOU BRD service, etc.), if they do not conflict with the latter.

#### **3.5.1.2. Subscriber**

The Subscriber is the Client who subscribes to a remote banking service.

The Account Proxy may also subscribe to some of these services. In this case, the contractual provisions applicable to the Subscriber shall also apply to the Account Proxy, subject to the limitations specified.

#### **3.5.1.3. General Conditions Regarding Eligible Accounts**

The accounts through which the Subscriber subscribes to the remote banking service must meet all of the following conditions:

- a) to be active;
- b) not be subject to any restrictions under the Bank's internal rules (e.g. being listed in the Payment Incidents Register or the Client being included on an international sanction list);
- c) must not be subject to any court-ordered restrictions (e.g. garnishment or seizure);
- d) not be blocked.
- e) to be opened at BRD in the name of an individual;
- f) the type of account is eligible for enrolment in the service;
- g) the Bank has not prohibited or restricted access to these accounts through remote banking services.

The Bank may restrict access to remote banking services if the accounts through which the Subscriber subscribed to these services no longer meet the above conditions or if the Bank identifies risks related to financial crime that are unacceptable to the Bank.

#### **3.5.1.4. Remote Banking Service Account**

The Subscriber must designate one of the accounts enrolled in the remote banking service as the service account. The Bank charges the fees related to the use of the service to this account. The types of accounts that may be designated as service accounts are communicated to the Subscriber when the service is contracted.

#### **3.5.1.5. Rights and obligations specific to Remote Banking Services**

##### **3.5.1.5.1. Rights of the Bank:**

- (a) To set limits on the value of transactions ordered by the Subscriber (per transaction and per day) and to modify such limits. They are communicated to the Subscriber through the remote banking service used by the Subscriber and may be consulted before each transaction is carried out.
- (b) To add new functionalities to the remote banking services without the need to enter into an addendum. If the Subscriber considers that the new functionalities are contrary to their interests, they may request termination of the agreement for the relevant service.
- (c) Not to intervene in disputes between the Subscriber and the telephone operator or Internet provider.
- (d) The Bank shall not be liable for, or pay compensation for, any direct or indirect damages incurred by the Subscriber or any other person in the following situations:
  - (d.1) fraudulent or other infiltration by third parties into the IT system of the telecommunications operator or internet service provider, resulting in the corruption of information, destruction of databases or software, or disclosure of information. The telecommunications operator/internet service provider remains solely responsible for the protection and security of its IT system;
  - (d.2) complaints or malfunctions caused by the fault or negligence of the telecommunications operator/internet service provider or its subcontractors;
  - (d.3) any incidents affecting the transmission of information over the telecommunications operator's/internet service provider's network when the Subscriber uses the services;
  - (d.4) loss of data, distortion or delays in data transmission caused by events beyond the Bank's control;

- (d.5) failure to comply with the Bank's instructions, incorrect information entered by the Subscriber when carrying out transactions, or malfunction of the Subscriber's equipment;
- (d.6) service malfunctions beyond the Bank's responsibility;
- (d.7) interruption of the remote banking service if the Subscriber does not contact the Bank to carry out transactions through other services made available by the Bank;
- (d.8) the Subscriber's use of unsecured remote communication methods, which may lead to fraud.

#### **3.5.1.5.2. Bank's Obligations:**

- a) to apply Strong Customer Authentication when the Client accesses their payment account online, initiates an electronic payment transaction, or carries out any action through a remote channel that may involve a risk of payment fraud or other abuse.
- b) to be liable for losses incurred by the Subscriber because of: (i) transactions carried out after the Subscriber has notified the Bank that third parties are aware of the Subscriber's Personalised Security Credentials; (ii) transactions carried out contrary to the instructions given by the Subscriber;
- c) to provide the Subscriber with a detailed list of transactions carried out in the current/revolving accounts through the remote banking service;
- d) to promptly take the necessary measures to assess, prevent and limit the risks of fraudulent use of the Personalised Security Credentials if the Subscriber notifies the Bank of any of the events referred to in Article 3.5.1.5.4(d).

#### **3.5.1.5.3. Subscriber's rights**

The Subscriber may change the service account and the list of accounts available for use through the remote banking service, provided that at least one eligible account is maintained.

The changes may be made • at the Bank's branches, by completing the relevant forms, • through the MyBRD service, or • by other means made available by the Bank.

Removing an account from the list of eligible accounts does not affect the existence of that account.

#### **3.5.1.5.4. Subscriber's obligations:**

- a) To keep and use securely the personalised Security Elements for each remote banking service. They are solely responsible for the consequences of their disclosure or use by third parties.
- b) Do not define/use Custom Security Elements that can be easily guessed or identified by third parties.
- c) To immediately inform the Bank of any unauthorised disclosure or use of the Personalised Security Elements.  
Transactions performed by the Subscriber must be authorised based on personalised Security Elements. Entering the Subscriber's Personalised Security Elements constitutes the Subscriber's irrevocable consent to the processing of the submitted transactions. The Bank shall not be liable for the consequences thereof.
- d) To notify the Bank immediately if they notice transactions in their account that he did not order or if he suspects that other persons know the Personalised Security Elements.
- e) To designate a service account from which the Bank will debit the fees and costs related to the transactions carried out. If this account becomes inaccessible through the remote banking service, the Subscriber must designate another service account.
- f) To periodically review the information and guidelines on the use of the service published on the Bank's website and available at its branches.

#### **3.5.1.6. Provision by third parties of the information services on accounts or payment initiation**

The provision of these services by third parties is not conditional on the existence of a contractual relationship between them and the Bank.

The Bank may grant such third parties access to the Client's online-accessible account but shall not be responsible for the performance of their obligations.

The Bank may deny a PISP or AISP access to a payment account if there are objectively justified reasons and evidence of unauthorised access to the account by such PISP or AISP. In such cases, the Bank shall inform the Client (through the means agreed under the Contract) of the refusal of access to the payment account and the reasons for such refusal.

##### **3.5.1.6.1. Payment initiation services**

The procedure for expressing the consent for the execution of a payment transaction is the one agreed between the Client and PISP. The Bank communicates securely with the PISP. Immediately upon receipt of the payment order from the PISP, the Bank shall provide the PISP with all the information necessary for the execution of the transaction.

The Bank shall not charge the Client different fees for transactions initiated in this manner.

##### **3.5.1.6.2. Account information services**

The procedure for expressing the consent for the supply of information related to the Client's accounts opened with BRD is the one agreed between the Client and AISP.

The Bank communicates securely with the AISP and provides it with information on the Client's online-accessible accounts.

The Bank shall not charge the Client any fees in connection with this service.

##### **3.5.1.7. Remote banking services fees**

The Subscriber is required to pay the monthly administration fee for the remote banking service and the fees/costs related to transactions carried out through that service, in accordance with the Fee Guide.

The Subscriber also bears the cost of telephone communication and internet service. This will be billed directly by their telephone operator or internet provider.

##### **3.5.1.8. Duration, suspension, termination of the contract**

**Duration.** The contract regarding remote banking services is concluded for an indefinite period.

**Suspension and termination.** In addition to the cases in Article 1.8., the Bank may suspend access to the remote banking service and, where applicable, terminate the Contract related thereto, without prior notice or other formality, in the following situations:

- a) eligible accounts no longer meet the conditions referred to in article 3.5.1.3.;
- b) The Subscriber fails to maintain sufficient funds to pay the monthly administration fee or other costs due for using the service, according to the Contract;
- c) The service account is deleted from the list of eligible accounts and there is no other account that could become a service account;
- d) risks arise related to the security of the Bank's information system;
- e) The subscriber does not comply with the provisions of the Contract regarding remote banking services.

**The subscriber** may request the suspension or termination of the remote banking services agreement • in writing, at the Bank's branches, or • by telephone, through the MyBRD Contact service.

##### **3.5.1.9. Other provisions regarding remote banking services**

The records of the systems used to receive the Subscriber's instructions and reproductions thereof in electronic or paper form (e.g. printed account statements) constitute conclusive evidence that the Bank has received the Subscriber's instructions. They constitute evidence supporting the execution of the transactions and the charging of the related fees.

In accordance with the law, these instructions shall be retained on the Bank's servers for 10 years from the end of the financial year in which they were issued.

The general, economic and financial information provided through the remote banking services is for informational purposes only.

The content of the websites and the software supporting the remote banking services are the exclusive property of the Bank. Any use

thereof without the Bank's prior consent (e.g. by reproduction, adaptation, representation, etc.), other than as permitted under the Contract, is prohibited and subject to penalties in accordance with the law.

### 3.5.2. MyBRD Contact service

**3.5.2.1.** It is a remote banking service provided via telephone. It can be accessed by calling the following telephone numbers:

- 021 302 61 61 – standard-rate number, available from any network;
- \*BANCA (\*22622) – charged at the same rate as an on-network call, from any Orange, Vodafone, Telekom Mobile or RCS Digi Mobil number.

**3.5.2.2.** Through this service, the Subscriber may securely obtain personalised information on their account balances and the latest transactions recorded on their accounts, automatically via the automated telephone system.

The Subscriber selects the option corresponding to the desired information using the telephone keypad and follows the instructions provided by the automated telephone system.

The Subscriber is identified using the MyBRD Contact Identifier and the Numeric Access Password.

**3.5.2.3. Activation.** The service becomes active:

- a) if contracted at a BRD branch – on the second business day following the signing of the Bank's standard forms;
- b) if contracted through MyBRD Contact – upon the Subscriber's telephone confirmation.

**3.5.2.4.** Termination of the service shall take effect on the second business day following the date of the request.

**3.5.2.5. Eligible Accounts.** Through this service, the Subscriber may obtain information about current, or savings accounts opened with the Bank in their name or for which they are an authorised representative.

For the Subscriber to enrol in this service with accounts for which they are an authorised representative, the account holder's consent must be given at a BRD branch.

### 3.5.3. MyBRD SMS Service

**3.5.3.1. Service Description.** It is a remote banking service accessible via mobile telephone at the short number 1701. It allows the Subscriber to obtain information about accounts held with the Bank and general banking information.

**3.5.3.2. The information available through the MyBRD SMS service** includes:

**a) Information about accounts** opened at the Bank:

- for **current and savings accounts**: • the date and time the balance information was sent (day, hour, minute), • the account label and currency, • the available balance at that time, • the approved credit limit;
- for **accounts with an attached credit card**: • the date and time the balance information was sent (day, hour, minute), • the account label and currency, • the available balance at that time, • the credit due date, • the interest rate;
- for **credit accounts**: • balance transmission date (day, hour, minute), • account label and currency, • account balance (credit balance + arrears), • credit due date, • interest rate;
- for **deposit accounts**: • the date and time the balance information was sent (day, hour, minute), • the account label and currency, • the available account balance, • the deposit maturity date, • the interest rate.

**b) Information on the last 5 transactions (mini-statement of account)** from a current account, savings account or account linked to a credit card: • debit transactions, • credit transactions.

**c) Predefined alerts** regarding changes in the balance of current and savings accounts:

- an increase in the balance above a predefined threshold or a decrease below a predefined threshold;

- the account being debited or credited with an amount exceeding a predefined threshold.

**d) Alert management:** The Subscriber may add, delete or list alerts using their mobile phone.

**e) Information on the Bank's exchange rates** and the NBR exchange rates for the following currencies: USD, EUR, GBP, CHF and JPY. Information may also be provided for past dates, but no more than one year prior to the date of the request.

**f) General information** on the Bank's range of services and products.

**g) Other functionalities** to be launched by the Bank at a later date (future).

**3.5.3.3. Terms of Use.** To use the MyBRD SMS service, the Subscriber must have a mobile phone connected (under a subscription or prepaid plan) to the network of a Romanian mobile network operator licensed to provide GSM services. The service may be used in Romania and in countries where the mobile network operator has roaming agreements in place (provided that the Subscriber has activated the roaming service).

**3.5.3.4. Eligible Account Types and Functionalities.** The account types that may be used and the functionalities of the MyBRD SMS service are communicated to the Subscriber before the agreement is entered into. They may subsequently be changed by the Bank, subject to prior notice to the Client.

The Subscriber may subscribe to MyBRD SMS with new accounts • at the Bank's branches or • by telephone, via the MyBRD Contact service.

**3.5.3.5. Support account.** To subscribe to MyBRD SMS, the Subscriber must designate at least one active account that can be used via MyBRD SMS and that will serve as the Service's support account. This account must be a current account, savings account or an account with an attached credit card. The Subscriber may subsequently request that this account be changed.

**3.5.3.6. How to use.** Through the MyBRD SMS Service, the Subscriber may obtain information on the status of the accounts registered for the Service at any time, 24 hours a day, 7 days a week. The Subscriber may obtain this information as follows:

- a) on request: by sending an SMS command to the short code 1701;
- b) periodically: at a predefined frequency (daily, weekly, monthly) – for information on the balances of accounts that can be used through this service and on exchange rates;
- c) by generating predefined alerts.

**3.5.3.7. Security Code (PIN).** The first time the Subscriber accesses MyBRD SMS, a security code (PIN) provided by the Bank upon activation of the service must be used. This is a randomly generated alphanumeric code. For subsequent access to the service, the Subscriber must change this code.

The PIN may be entered using either lowercase or uppercase letters. The Subscriber must keep the PIN confidential.

If the Subscriber enters an incorrect PIN three consecutive times, access to the service will be suspended as a security measure. In this case, the Subscriber must contact the Bank to have the PIN reset (at any Bank branch or by telephone, via the MyBRD Contact service).

**3.5.3.8. The Bank shall not be liable** in the following cases:

- a) the mobile phone is not operational due to non-payment of the telephone bill or failure to fulfil other obligations towards the mobile network operator;
- b) The Subscriber does not receive messages because the mobile phone or mobile network is not operational, or the Subscriber is outside the mobile network operator's coverage area;
- c) loss of integrity of the data correctly and completely transmitted by the Bank, due to the fault of telecommunications service providers;
- d) The Subscriber is unable to send or receive messages on the mobile phone due to the phone settings configured by the Subscriber or imposed by the mobile network operator;

- e) The Subscriber enters incorrect information using the mobile phone keypad.

#### **3.5.3.9. Other obligations of the Subscriber:**

- (a) to purchase, at the Subscriber's own expense, a mobile phone compatible with the MyBRD SMS Service and ensure that it is operational and connected to a mobile network operator;
- (b) to keep the mobile phone and SIM card safe. The Bank shall not be liable for transactions carried out in the event of their loss, theft or lending;
- (c) to immediately request that the mobile network operator block the SIM card in the event of loss or theft of the mobile phone or SIM card;
- (d) to immediately inform the Bank of any situation that could prevent access to messages (e.g. loss or theft of the mobile phone or SIM card, change of telephone number, termination of the agreement with the mobile network operator, etc.). otherwise, the Bank will continue to send messages to the telephone number provided by the Subscriber in the MyBRD SMS Service subscription documentation;
- (e) to pay the service charges detailed below.

**3.5.3.10. Charges.** For using the MyBRD SMS service, the Subscriber must pay the following fees to the Bank:

- a) monthly administration fee:** charged monthly to the support account on the 1st day of the month for use of the service during the previous month;
- b) balance inquiry and mini-statement fee** for current accounts, savings accounts and accounts with an attached credit card. It is charged to the account for which the information was requested, before the information is sent;
- c) fee for messages received,** such as: alerts, balances of deposit and credit accounts, exchange rate inquiries, general information. It is charged monthly to the support account on the 1st day of the month for messages received during the previous month.

The amount of these fees is published in the Fee Guide.

**3.5.3.11.** The cost of SMS messages sent by the Subscriber is determined by the mobile network operators and is payable in accordance with the agreements entered into with them.

**3.5.3.12.** Transactions carried out on the accounts registered by the Subscriber for the MyBRD SMS service and the related bank fees are shown on the account statement. At the Subscriber's request, the Bank will provide a detailed list of the transactions carried out.

### **3.6. ACCOUNT SWITCHING SERVICE**

#### **3.6.1. General Provisions**

It is a service whereby the Account Holder may switch from one payment service provider (referred to as the "Previous Bank") to another (referred to as the "New Bank"):

- a) information on all or some of the standing orders for credit transfers, recurring direct debits and recurring incoming credit transfers executed on a current account; and/or
- b) the positive balance of the payment account (to another payment account).

The switch may be made with or without closing the previous account.

It may only be carried out between payment accounts denominated in the same currency.

For the switch, the Account Holder does not need to contact the Previous Bank. The Account Holder must complete and sign a form (the "Authorisation"), requesting the Previous Bank and the New Bank to carry out the operations necessary for switching the account. BRD may act as either the New Bank or the Previous Bank.

#### **3.6.2. The switching accounts service on national territory**

**3.6.2.1.** If the **Bank acts as the New Bank**, it will open the Account only after receiving the Authorisation and after the contractual account-opening documentation has been signed.

Under the Authorisation, the Client may:

- a) authorise the **Previous Bank to:**

- (a.1) provide the New Bank (and the Client, at the Client's request) with a list of • the existing standing orders for credit transfers and • the direct debit mandates being switched;
- (a.2) provide the New Bank (and the Client, at the Client's request) with the available information on • recurring incoming credit transfers and • direct debits initiated by payees and executed on the Client's payment account during the previous 13 months;
- (a.3) stop accepting direct debits and incoming credit transfers from the date specified in the Authorisation;
- (a.4) cancel the standing orders from the date specified in the Authorisation;
- (a.5) transfer the remaining positive balance in the Client's payment account to the payment account opened with the New Bank, on the date specified by the Client;
- (a.6) close the payment account held with the Previous Bank, on the date specified by the Client.

- b) authorise **the New Bank to:**

- (b1) set up the standing orders for credit transfers requested by the Client and execute them from the date specified in the Authorisation;
- (b2) make the necessary arrangements to accept direct debits from the date specified in the Authorisation;
- (b3) inform the payers (specified in the Authorisation) making recurring credit transfers to the Client's account of the details of the Client's payment account opened with the New Bank; provide these payers with a copy of the Authorisation confirming the Client's consent to the account switch;
- (b4) inform the payees (specified in the Authorisation) collecting funds from the Client's payment account by direct debit of the details of the payment account opened by the Client with the New Bank and the date from which funds will be collected from this account; provide these payees with a copy of the Authorisation.

- c) determine which incoming credit transfers, standing orders for credit transfers and direct debit mandates are to be switched;

- d) specify the date from which standing orders for credit transfers and direct debits are to be executed using the payment account opened with the New Bank.

**3.6.2.2.** If the **Bank acts as the Previous Bank**, upon receiving a request from the New Bank, it will carry out the following operations, if provided for in the Authorisation:

- a) provide the New Bank with a list of • the existing standing orders for credit transfers and • the direct debit mandates being switched;
- b) provide the New Bank with information on • recurring incoming credit transfers and • direct debits initiated by the creditor and executed on the Client's payment account during the previous 13 months;
- c) stop accepting incoming credit transfers and direct debits from the Client's payment account from the date specified in the Authorisation;
- d) cancel the standing orders from the date specified in the Authorisation;
- e) transfer the remaining positive balance in the Client's payment account to the Client's payment account opened with the New Bank, on the date specified in the Authorisation;
- f) closes the payment account on the date specified in the Authorisation.

By way of exception, **the payment account is not closed if:**

- The client has outstanding obligations in relation to that payment account;
- the account is used for other active services contracted by the Client (e.g. loans, cards, deposits, remote banking services, etc.); or

- the account is seized or blocked, according to the law, for obligations assumed by the Client towards the Bank or third parties.

**The account is closed only if the following cumulative conditions are met:**

- The Client has handed over to the Bank all instruments and devices through which the Account is accessed; and
- the conditions regarding the closure of the account and the attached products and services are met, according to the contract concluded between the Client and the Bank.

### **3.6.3. Assistance for opening a payment account in another EU Member State**

If the Client wishes to open a payment account with a New Bank located in another Member State of the European Union, upon receiving the Client's request, the Bank will provide assistance as follows:

a) provides the Client, free of charge, with:

- a list of • the standing orders for credit transfers active at that time and • the direct debit mandates set up by the Client; and
- the available information on recurring incoming credit transfers and direct debits initiated by payees and executed on the Client's payment account during the previous 13 months;

b) transfers the remaining positive balance in the Client's payment account to the Client's payment account opened with the New Bank, provided that the request contains complete information allowing the New Bank and the payment account to be identified;

c) closes the payment account held by the Client.

By way of exception, **the payment account is not closed** if:

- The customer has outstanding obligations in relation to that payment account;
- the account is used for other active services contracted by the Client (e.g. loans, cards, deposits, remote banking services, etc.); or
- the account is seized or blocked, according to the law, for obligations assumed by the Client towards the Bank or third parties.

**The account is closed only if the following cumulative conditions are met:**

- The Client has handed over to the Bank all instruments and devices through which the Account is accessed; and
- the conditions regarding the closure of the account and the attached products and services are met, according to the contract concluded between the Client and the Bank.

## **4. PRODUCT AND SERVICE PACKAGES**

**4.1. Definition.** Product and service packages are combinations of products and services based on a support account. The products and services included in the package retain their specific terms and conditions of operation.

**4.2. Package Support Account.** This is the current account through which transactions relating to the products and services included in the package are carried out. The basic payment account may serve as the package support account only if the Client waives the fee-related benefits of the basic payment account and accepts the benefits and other terms and conditions of the package.

**4.3.** At the Client's request, products and services offered by the Bank other than those included in the package may also be linked to the package support account. They are contracted separately from the package, operate as individual products and are subject to standard fees and charges.

**4.4.** A product or service may not be included simultaneously in more than one package held by the same Client (except for the MyBRD Contact, MyBRD SMS and YOU BRD services).

### **4.5. Package benefits**

**4.5.1.** The Bank may offer **preferential pricing terms** to package holders:

- a) for the products included in the package (compared to purchasing them individually); and, where applicable,
  - b) for other products or services offered by the Bank that they hold.
- In this case, the preferential pricing terms apply for as long as the package is held, starting from the first due date for such charges following the purchase of the package.

**4.5.2.** The Client holding the package may also have access to **certain non-banking benefits** negotiated by the Bank with external partners. These may change and are periodically updated in promotional materials and on the website [www.brd.ro](http://www.brd.ro).

**4.5.3.** The benefits associated with the package **cannot be combined** with those provided under a salary or other monetary entitlements payment agreement.

**4.6. Purchasing the package.** The Client may purchase a product and service package through BRD branches, online, or via the MyBRD Contact service. For this purpose, the Client must provide the required information and indicate their choices in the specific forms made available by the Bank, either in paper or electronic format, and complete the contracting process applicable to the chosen contracting channel.

**4.7. Package Agreement.** The Package Opening Form, together with the General Banking Conditions, the Fee Guide and the agreements specific to the products/services included in the package, including their annexes, constitute the Package Agreement.

### **4.8. Package Fees**

**4.8.1.** Throughout the term of the package, the Client shall pay the fees and charges applicable to the package, as set out below. These are automatically charged to the package support account when due. If there are insufficient funds available in the package support account, they will be charged to any other account held by the Client.

#### **4.8.2. Monthly Package Administration Fee**

**4.8.2.1.** This fee includes: • the monthly administration fee for the account or accounts included in the package; • the annual administration fee for the debit card included in the package; • the monthly administration fee for remote banking services, where applicable; • the fees for transactions included free of charge in the package. The amount of the fee is specified in the package opening documentation.

**4.8.2.2.** For certain packages, the **monthly package administration fee is 0 (zero) if certain conditions** specified in the package opening documentation **are met**. These conditions may consist of one or more of the following:

- a) **minimum incoming payments.** "Incoming payments" means amounts credited to the current or savings accounts held by the Client with BRD. By way of exception, when verifying this condition, the amounts originating from: • loans granted by the Bank, • deposits that have reached maturity, • credit transfer operations carried out between own accounts opened with the Bank, • credit transfer operations representing returns of funds (partial or total) of transactions carried out with the card are not taken into account;
- b) **holding funds within the BRD Group.** "Funds" means the balance held at the end of the month in current accounts, savings accounts, term deposits and investment products;
- c) **making a minimum number of payment transactions** each month (by the end of each month). Only the following payment transactions are taken into account when verifying whether this condition is met:
  - payments made via the YOU BRD service from any current account held by the Client with the Bank, comprising • intrabank payments (except for payments between accounts held by the same Client), • intrabank payments involving financial instruments, • instant or standard interbank

payments (including payments to the State Treasury), • bill payments; and

- payments made with the debit card included in the package: • at Merchants' POS terminals, including online payments (excluding quasi-cash transactions), and • card payments of bills at ATMs/MBAs/ROBO terminals;

**d) maximum age** of the package holder.

**4.8.2.3. Grace Period.** If a grace period is specified in the package opening documentation:

- during this period, the Client does not pay the monthly package administration fee, regardless of whether or not the conditions mentioned above are met;
- after the grace period expires, the Bank will verify whether these conditions are met. If the conditions are not met, the Bank will automatically charge the monthly package administration fee applicable to the type of package held to the package support account.

**4.8.2.4. For current account packages not subject to the conditions** referred to in Article 4.8.2.2, the monthly package administration fee is charged each month on the day corresponding to the date on which the package was purchased.

**4.8.2.5.** If, during certain periods, the Bank does not exercise its right to charge the monthly package administration fee, this does not constitute a waiver by the Bank of its right to charge this fee in the future.

**4.8.3. Annual Premium for Confort Insurance.** If the package includes insurance taken out prior to the purchase of the package, the preferential premium will be charged on the next annual due date.

**4.9. Change of the products and services package structure.**

The Bank has the right to modify the structure of the product and service packages contracted by the Client. Accordingly, it may remove or replace certain products included in the package if they are no longer offered by the Bank. Any change to the structure of the packages will be communicated to the Client and will take effect on the date specified in the relevant notice.

**4.10.** The Client may request the **replacement of the product and service package held with another package** at the Bank's branches or, for certain packages, via the MyBRD Contact service. The previous package is closed, and a new package is opened in its place.

The products and services included in the previous package:

- (i) if they are included in the structure of the new package, they will be included in it. They will be subject to the pricing terms applicable to the new package;
- (ii) if they are not included in the structure of the new package, they will become subject to the standard pricing terms in force on the date the package is closed. The Client may close them, if they wish, in accordance with the specific features and documentation applicable to each of them.

**4.11. Closing product and service packages**

**4.11.1.** Either Party has the right to terminate the Product and Service Package Agreement unilaterally, subject to prior written notice to the other Party. This notice period is at least: • 30 calendar days (for termination by the Client) and • two months (for termination by the Bank), respectively.

**4.11.2.** The package may be closed • at the Bank's branches, • (for certain packages) via the MyBRD Contact service, or • by completing the dedicated form made available by the Bank on its

institutional website [www.brd.ro](http://www.brd.ro). Upon termination of the package, the Client may:

- a) terminate all products included in the package; or
- b) retain one, several or all of the products included in the package as standalone products (if they are also available individually in the Bank's product offering, outside the packages). For the products and services retained, the Bank's standard fees and interest rates in force at the time the package is closed will apply.

**4.11.3.** In the event of unilateral termination by the Client, the Package Agreement will terminate only after all due and outstanding payment obligations arising from it have been settled.

**4.11.4.** The Bank may terminate the package or any product/service included in the package if the Client fails to pay the related fees and charges or fails to comply with other obligations undertaken under the agreement.

**4.12. Closing products and services within the package**

**4.12.1.** A product or service included in the package may be closed by the Client, upon request, or by the Bank, in accordance with the provisions of the Agreement.

**4.12.2.** If products or services included in the package are closed, this may or may not result in the closure of the package, as follows:

**a) The closure of a product/service that is mandatory for the package results in the closure of the package.** The following are mandatory in the package:

- (i) support account;
- (ii) the primary debit cards linked to the support account, issued in the name of the package holder and purchased as part of the package (including those issued/renewed and not collected within the agreed period);
- (iii) MyBRD Contact and MyBRD SMS services (if mentioned as mandatory in the package opening documentation);
- (iv) certain free benefits included in the package.

After a mandatory product or service and the package are closed, the other products and services included in the package remain active. Starting from the next due date, they will be subject to the fees applicable to products or services purchased separately (outside a package), in accordance with the Fee Guide.

**b) The closure of products/services that are optional within the package does not result in the closure of the package.** The following are optional within the package:

- (i) current accounts additional to the package support accounts;
- (ii) additional debit card for the package holder;
- (iii) the debit card for the Authorised User designated by the holder;
- (iv) savings account;
- (v) MyBRD SMS, MyBRD Contact services (if mentioned as optional in the package opening documentation);
- (vi) YOU BRD Service,
- (vii) Comfort insurance.

After these products and services are closed, the package remains active and the Bank continues to charge the package administration fee in accordance with the Fee Guide.

## **ANNEX. 'INFORMATION ON THE PROCESSING OF PERSONAL DATA;**

In this Annex, B.R.D. - Groupe Société Générale S.A. (the "Bank" or "we"), in its capacity as data controller, informs you how we process<sup>2</sup> your personal data in the context of the activities carried out by the Bank, as well as about your rights as a data subject.

### **I. WHAT DATA CATEGORIES DO WE PROCESS?**

<sup>1</sup>Prepared in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC ("GDPR"), applicable as of 25 May 2018.

<sup>2</sup>Processing means any operation performed on personal data (such as collecting, recording, organising, storing, consulting, using, disclosing, copying, erasing or destroying such data). Personal data means information that identifies or may lead to the identification of a natural person.

Where applicable, the Bank processes the following categories of personal data:

- **identification data**, for example:
    - data contained in identification documents (identity card, birth certificate, passport, residence permit, etc.): surname, first name, Personal Numerical Code (CNP), series and number of the identification document, date and place of birth, citizenship, sex, type of identification document, date of issue, expiry date, etc.;
    - signature;
    - personal data contained in the digital certificate, if you use an electronic signature in your relationship with the Bank;
    - data contained in the document (birth certificate/court decision) certifying the status of legal representative of a minor/person lacking legal capacity or having limited legal capacity.
  - **civil status data**: data from the marriage certificate, etc.
  - **contact details** such as: home address, mailing address, email, phone.
  - **video or still images**, when:
    - entering into a relationship with the Bank or contracting products/services does not require your physical presence at our branches;
    - visit the Bank's offices; or
    - use our ATMs.
- Our surveillance system does not capture images through focusing, selective targeting or profiling. Records are processed continuously or sequentially.
- **the voice**, when:
    - entering into a relationship with the Bank or contracting products/services does not require your physical presence at our branches;
    - we record telephone calls (e.g. in the cases described under point D of Chapter III below); or
    - you participate in teleconferences or videoconferences in connection with the performance of the agreement, only if you have consented to the recording of your voice and the data communicated during that conference.
  - **the photo** from the identity card/identification document;
  - **data required to verify your eligibility**, for example:
    - information regarding your professional status (occupation, employer's name, position held, etc.);
    - information required for know-your-customer (KYC) purposes (public office held, politically exposed person status, special relationships with the BRD Group, etc.);
    - tax information (country/countries of tax residence, tax identification number, etc.);
    - information about your financial and economic situation (income, solvency, credit history, assets owned, etc.);
    - transactional information (transaction history, type of banking product held, date of granting/maturity, initial or current amounts/balances, outstanding amounts, garnished amounts, etc.);
    - information regarding fraudulent or potentially fraudulent activities (allegations and convictions for fraud/attempted fraud, misdemeanours or criminal offences, including money laundering or terrorist financing, etc.);
    - data relating to collateral, e.g. information regarding the original owners of the property provided as collateral, etc.;
    - health data: • data contained in documents issued by the healthcare institution certifying the costs of treatment, hospitalisation, medical investigations or procedures (in the case of loans for medical expenses); • documents issued by the General Directorate of Social Assistance and Child Protection (in the case of loans for the purchase of vehicles adapted for persons with disabilities or for adapting a home

to the specific needs of persons with disabilities);

- **any other data necessary or useful for carrying out the Bank's activities**, in accordance with the law; as well as
- **data provided by data subjects** in their interactions with the Bank.

**Note:** In the case of clients represented by other persons (attorneys-in-fact, legal representatives, etc.), the Bank also processes the identification data of the person representing the client, such as: surname and first name, date and place of birth, Personal Numerical Code (CNP) or a similar identifier, residential address and its legal status (domicile, residence), citizenship, and other personal data specified in the document establishing the authority to represent the client.

## II. WHERE DO WE GET THE PERSONAL DATA FROM?

We process personal data that:

- you provide to us, directly or indirectly (through other persons acting on your behalf), or
- we generate or infer because of our interactions with you through any communication channel;
- we obtain from external sources, such as:
  - a) **public institutions and authorities**, for example: • the National Agency for Fiscal Administration (ANAF), • the National Credit Guarantee Fund for SMEs (FNGCIMM), • the Central Credit Register (CRC), • the Payment Incidents Register (CIP), • the National Integrity Agency, • the National Public Pension House, • the General Directorate for Persons Records, etc.  
These institutions/authorities may provide us with information such as: your tax status, including your tax identification number; your declaration of assets, in the case of publicly exposed persons; the status of your enforcement proceedings; your employment status; the status of your compensation claim with FNGCIMM; data from the Central Credit Register, including your identification data, information on the type of loan taken out, your level of indebtedness and membership of a group of debtors.
  - b) **electronic registers and databases**, for example: • the Courts Portal, • the Credit Bureau, • RNPM, • databases of persons subject to international sanctions and politically exposed persons, • R.N.E.P.; (National Register of Persons Records), etc. We check these sources when you enter into a relationship with the Bank or when you apply for financial and banking products and services. For example, we consult:
    - R.N.E.P. to verify the data you provide to us and to obtain additional information about your identity. Such data includes, for example: surname, first name, Personal Numerical Code (CNP), type, series and number of the identification document, domicile/residence address, date of issue, expiry date and issuer of the identification document, date and place of birth, your photograph from the identification document, etc.;
    - the Courts Portal, to verify whether you are involved in criminal proceedings that may indicate fraudulent conduct;
    - The Credit Bureau, if you apply for a credit product, to obtain information about your payment behaviour and any incidents in your dealings with other financial institutions;
    - databases of persons subject to international sanctions, to verify whether you are included in such databases.
  - c) **entities involved in payment transactions**, for example: • international card organisations (Visa, Mastercard, etc.), • merchants that accept card payments, • banks and other financial institutions involved in payment schemes, • the Central Depository, etc. For example:
    - when you make card transactions, we receive the data necessary to process the payments (card details, transaction

amounts, etc.) from the merchants where you make card payments;

- when you carry out other payment transactions (by credit transfer, direct debit, cheque, bill of exchange or promissory note), we receive your data from the financial institution where the transaction was initiated, through payment schemes/systems and interbank communication systems (SEPA, Regis, SENT, SWIFT, etc.).

- d) **commercial partners**, particularly service providers for the Bank. For example, we may obtain your contact details (address, telephone number, etc.) from debt collection agencies that work with us.
- e) **healthcare institutions**: public or private clinics or hospitals, the General Directorate of Social Assistance and Child Protection, other institutions that provide medical treatment or subsidise loan repayments for persons with disabilities, etc.
- f) publicly accessible **online platforms** (social media, the Internet) and data aggregators.
- g) **entities within the BRD Group** (for example, data concerning clients who have had agreements with BRD Finance IFN S.A.).
- h) **your employers**, for example, if we enter into a salary payment agreement with your employer.
- i) **companies for which the Bank provides payment services** (securities issuers, insurance companies, etc.).
- j) **certificate issuers**, if you use electronic signature.
- k) **Central Depository** (registrar for the Bank's shares).
- l) in certain situations, we may receive data from (i) **the Bank's clients and their representatives** (e.g. if you are a family member of a client), or (ii) **members of the Bank's management bodies** (if you are a person affiliated with them).

Your refusal to provide us with your personal data may result in the rejection of your request to enter into a relationship with the Bank or to contract certain products or services.

### III. WHY (FOR WHAT PURPOSE) DO WE PROCESS PERSONAL DATA?

#### A. ENTERING INTO A RELATIONSHIP WITH THE BANK

We process personal data:

- a) to verify whether you are eligible to enter into a relationship with the Bank and to contract banking products or services; and
- b) to prepare the documentation required for contracting the requested product or service.

We assess your circumstances to ensure that you meet the applicable requirements, in accordance with the law and the Bank's internal policies (including its risk policies). For example:

- in applying know-your-customer procedures, we process data such as: surname, first name, date and place of birth, type and country of issue of the identification document, Personal Numerical Code (CNP), series and number of the identification document, domicile and residence address, tax residence and tax identification number, telephone number, fax number, e-mail address, citizenship (including multiple citizenship, where applicable), source of funds, sector of activity, occupation and place of employment, purpose and nature of the relationship with the Bank, declared income range, status as a politically exposed person, family member of a politically exposed person or person known to be a close associate of a politically exposed person, public office held, etc.;
- we verify whether you meet the requirements regarding fraud prevention, anti-money laundering and counter-terrorist financing;
- we assess your circumstances and those of other persons, where applicable (co-borrowers, guarantors, etc.), in order to assess

the risk to which the Bank would be exposed by entering into the agreement for the product/service you request.

For certain products (e.g. credit products), we also use automated processing (including scoring) to verify whether you meet the eligibility requirements for entering into the agreement. Further details can be found in Chapter IV below.

**Note:** In the case of clients represented by other persons (attorneys-in-fact, legal representatives, etc.), the Bank also processes the representative's personal data necessary to identify them or to verify their authority to act on behalf of the client.

#### B. PROVISION OF FINANCIAL AND BANKING PRODUCTS AND SERVICES. PRODUCT AND SERVICE MANAGEMENT

We process personal data for the conclusion and performance of the contract with you. Therefore:

- For the **prevention and combating of fraud** and/or to **ensure banking secrecy**:
    - we verify the authenticity of the identification documents and other documents you provide to us;
    - we monitor the performance of the agreement and the associated risks;
    - we apply conflict-of-interest management procedures.
  - To **communicate with you about matters relating to the agreement or the banking product/service** contracted, we may contact you or, where applicable, other persons (co-borrowers, guarantors, attorneys-in-fact, legal representatives, etc.) through various channels, including by telephone, e-mail, SMS, at your home address, etc. For example:
    - if difficulties arise in the performance of the agreement, we may contact you to jointly identify solutions for continuing the contractual relationship under the best possible conditions;
    - we may send you notifications regarding payment due dates or changes to certain features of the contracted product/service.
  - For the **execution of payment transactions** that you initiate or of which you are the beneficiary and which are settled through Transfond, Transfond will generally have access to the following personal data: • IBAN, • beneficiary's surname and first name, • amount transferred, • payment details, • payer's surname and first name. This information is processed on a contractual basis for the purpose of executing the payment transaction.

The data transferred by the Bank to Transfond is also accessed by the other financial institutions participating in the payment scheme operated by Transfond, under legally secure conditions and in accordance with strict technical rules. The complete list of participants can be found at: <https://www.transfond.ro/pdf/List%C4%83ncilor%20care%20ofer%C4%83%20SANB.pdf>.
  - For certain payment services, we may act as **joint controllers together with Transfond**. We will specifically inform you about such services before they are implemented. Examples:
    - **RoPayP2P service** in proximity. This is a service for initiating instant payment requests by the payee, provided by financial institutions participating in the RoPay Payment Scheme. The list of these institutions is available on the Transfond website, at: <https://www.transfond.ro/servicii/casa-de-compensare-automata-sent>. The service is provided according to the set of rules regarding the RoPay Scheme, issued by Transfond. BRD is a participant in the RoPay Scheme;
    - the SANB service, described in the letter. H below.
- When we act as joint operators with Transfond:
- Your requests to exercise the rights referred to in Chapter VII below may be submitted to either BRD or Transfond. We will keep each other informed and provide mutual assistance to ensure that we respond to you within the statutory time limit (as a rule, one month). However, your main point of contact is the

Bank, at the address specified in Chapter VIII below. If you contact Transfond, it will redirect your request to BRD.

- If personal data protection incidents occur about which you must be informed, you will generally be informed by the Bank. The content of the information will be agreed in advance between the Bank and Transfond. More information about Transfond's processing of personal data, including the contact details of the Transfond data processing officer, can be found at: <https://www.transfond.ro/contact>.

- In order to carry out the contract with you, we also process your data for **archiving and storing email correspondence**.

### C. ECONOMIC-FINANCIAL AND ADMINISTRATIVE MANAGEMENT. ANALYSES AND INVESTIGATIONS FOR INTERNAL USE

We process personal data to organize and streamline the Bank's activity. Thus, the data is used for:

- organising the internal databases required for the activities of the Bank's structures and departments;
- improving the activity of the BRD network, BRD processes, products and services;
- organising, carrying out and efficiently managing debt collection and recovery activities;
- preventing and investigating fraud and suspected fraud in banking transactions;
- carrying out aggregate financial analyses regarding the performance of the BRD network and its staff, including its sales force;
- preparing aggregate reports on: • BRD's activity and performance in the financial and banking markets, and • BRD's exposure to other financial institutions;
- supporting the Bank's position in any investigations, administrative and judicial proceedings, litigation, etc. in which the Bank is involved;
- carrying out analyses, internal audit procedures and investigations, on our own initiative or following reports from third parties (including public authorities);
- managing inspections and investigations initiated by public authorities;
- developing and testing the IT applications and systems used to provide services to clients and support the Bank's activities;
- ensuring the security of IT systems;
- archiving documents in paper and electronic format and backing up electronic data.

### D. SUPPORT SERVICES AND COMPLAINTS MANAGEMENT

We process personal data to: • resolve your requests or those of others; and • provide you with additional information about our products and services. For example:

- we may contact you by telephone to respond to your requests;
- we may process data contained in the documents you provide to us in order to handle your requests or complaints (e.g. a request to update your data or block your card);

We audio-record our conversations with you for the following purposes:

- to improve the quality of our services;
- to document your requests and complaints regarding our products and services, as well as our responses;
- to document your consent, choices or preferences regarding a particular product or service.

If you do not wish the conversation to be recorded, you may contact us through other available channels (e.g. by e-mail, courier or post at our contact address). In this case, the actual handling of your request or complaint will not be affected, but the time required to resolve it may be longer.

### E. COMPLIANCE WITH THE LEGAL REQUIREMENTS AND INTERNAL RULES

We process personal data in order to comply with the legal obligations applicable to credit institutions.

**Reporting.** Based on our legal obligations, we submit reports to the relevant public institutions and authorities, such as:

- a) reporting to the National Agency for Fiscal Administration (ANAF) on persons subject to FATCA or CRS reporting requirements;
- b) daily reporting to the National Office for Prevention and Control of Money Laundering (ONPCSB) of cash transactions and external transfers, in accordance with legal requirements;
- c) reporting suspicious transactions to the National Office for Prevention and Control of Money Laundering (ONPCSB);
- d) reporting payment incidents to the Payment Incidents Register (CIP) of the National Bank of Romania (NBR);
- e) notifying ANAF or other competent authorities when persons or entities triggering reporting obligations are identified;
- f) reporting sanctioned persons or entities to the Office for the Implementation of International Sanctions;
- g) daily reporting to ANAF regarding the Central Electronic Register of Bank Accounts and Payment Accounts;
- h) reporting to ANAF in response to requests for information/documents received from it;
- i) obtaining a Tax Identification Number (NIF) from ANAF for non-resident clients who hold an account or safe deposit box, if they do not already have a NIF and do not provide it to the Bank when opening the account/renting the safe deposit box.

Failure to comply with reporting obligations constitutes an administrative offence for the Bank. You may request additional information from us at any time regarding the reports we submit pursuant to our legal obligations, unless the provision of such information is prohibited by law.

Under the law, we cannot enter into a business relationship or continue an existing relationship if we are unable to apply **customer due diligence measures**.

To comply with legal requirements on customer due diligence and anti-money laundering, we collect and process your identification data or other data from independent sources (e.g. public or private databases), including information regarding your status as a politically exposed person.

The processing of data for customer due diligence purposes also includes the processing of data relating to third parties, such as: authorised representatives, legal representatives of persons lacking legal capacity or having limited legal capacity (guardians, curators, etc.), guarantors, etc. Information about guarantors is taken into account in the risk score of the client whose obligations they guarantee.

For the purpose of fulfilling the Bank's legal obligations to maintain up-to-date information on its clients, we may update your existing data in our records using data obtained from the General Directorate for Persons Records ("DGEP").

Monitoring for customer due diligence and anti-money laundering purposes may also be carried out using **profiling mechanisms and automated decision-making processes**, including models based on artificial intelligence. These compare the Client's expected transactional profile (based on the information provided to the Bank when the relationship is established or the data is updated) with the Client's actual transactional behaviour. These profiling mechanisms are reviewed periodically to ensure that they remain effective and accurate.

As part of the Société Générale Group, we **exchange information with other Group entities** in order to ensure compliance with customer due diligence and anti-money laundering legislation (for reasons of public interest).

**Société Générale S.A. may act as a joint controller together with the Bank** for certain processing activities, such as:

- determining the data required for anti-money laundering analysis;
- validating data quality before carrying out the specific anti-money laundering process;
- developing the model used to identify potentially unusual transactions that must be analysed by us to determine whether they are suspicious from an anti-money laundering perspective;
- complying with regulatory obligations regarding the identification and reporting of suspicious transactions, etc.

You may request from either of the two controllers (the Bank and Société Générale S.A.) a copy of or details regarding the agreement between them concerning the processing of your personal data. The Bank collects and transfers to Société Générale S.A. only personal data about which you have been informed in advance.

If you submit a request to exercise your rights under Chapter VII below to either BRD or Société Générale S.A., they will keep each other informed and provide mutual assistance in order to respond within the statutory time limit (as a rule, one month). However, your main point of contact is BRD, using the contact details provided in Chapter VIII.

In the event of personal data protection incidents requiring you to be informed in advance, you will be informed by either BRD or Société Générale.

For the purpose of managing managerial **oversight and internal control** activities relating to banking transactions carried out within BRD, we may process your data in order to: • verify compliance with legal requirements; • identify and address any operational or other risks.

For operational **risk management purposes**, we may process your personal data in order to: • comply with our legal obligations regarding the management of operational risk exposure and the mitigation of reputational or financial risks; and • ensure the proper functioning of the Bank's processes.

We may process your personal data for the establishment and management of **garnishments** and for providing information on garnished amounts to enforcement bodies or authorities, in accordance with our legal obligations.

To comply with legislation on the **protection of persons, property and valuables**, we process personal data through security systems (closed-circuit television (CCTV), access control systems) or access logs. The data are retained for the periods required by applicable regulatory requirements. They may be made available to the authorities upon request, subject to the applicable legal requirements.

In addition to our legal obligations, we are also required to comply with several internal requirements of the Bank (or requirements established at Société Générale Group level) regarding reporting and internal or external audits. In certain situations, these may involve the processing of personal data.

## **F. PAYMENT OF DIVIDENDS TO BRD SHAREHOLDERS**

## **G. ENSURING THE SECURITY AND PROTECTION OF PERSONS, PREMISES, PROPERTY AND VALUABLES. PREVENTING AND COMBATING BREACHES OF LEGAL PROVISIONS AND CRIMINAL OFFENCES**

We use closed-circuit television ("CCTV") systems to ensure the security and protection of the Bank's premises and property and of persons, and to prevent criminal offences.

Video recordings are accessed only in justified circumstances, such as: • security incidents, • indications of unlawful activities, • complaints regarding unauthorised activities captured by CCTV cameras.

## **H. PREVENTING AND INVESTIGATING FRAUD OR OTHER INCIDENTS RELATING TO CASH TRANSACTIONS CARRIED OUT AT THE COUNTER OR THROUGH THE BANK'S EQUIPMENT (ATMs, ROBO, ETC.)**

We retain images of **cash transactions** (e.g. cash received or deposited at ATMs, etc.) carried out using the Bank's equipment or at the Bank's cash desks. These images are reviewed in the event of complaints regarding the total or partial failure to dispense the amounts withdrawn, incorrect cash deposits, etc.

Together with Transfond, as joint controllers, we process your personal data (first name, surname initial and IBAN) in order to provide the **Beneficiary Name Display Service (SANB)**. This service is available for electronic payments to accounts held with institutions in Romania that have joined SANB. Its purpose is to prevent fraud in the execution of payment transactions and to prevent undue payments. The data we transfer to Transfond are stored by Transfond and updated periodically until your relationship with BRD ends. They may be accessed by other SANB participants. The complete list of SANB participants is available at <https://www.transfond.ro/pdf/Lista%20b%C4%83ncilor%20care%20ofer%C4%83%20SANB.pdf>.

## **I. HANDLING COMPLAINTS AND REPORTS RECEIVED FROM DATA SUBJECTS WHERE ACCESS TO VIDEO RECORDINGS IS REQUIRED**

We may review images captured by CCTV equipment in order to handle reports and complaints received from data subjects, where necessary.

You can find information on the legal grounds for these processing activities and the retention period for your data in the framework document governing the processing of your data in the Bank-client relationship. This document is available on the BRD website here: <https://www.brd.ro/prelucrare-datelor-cu-caracter-personal>.

It supplements this Notice with details on the processing of personal data for purposes such as:

- direct marketing, commercial communications and the personalisation of offers and products (processing activities that we carry out only with your consent),
- conducting surveys, market research, analyses and other internal studies, and internal segmentation of the client portfolio (processing activities that we carry out based on the Bank's legitimate interests, unless you object to such processing).

## **IV. AUTOMATED INDIVIDUAL DECISIONS**

In our processes, we sometimes use automated individual decisions, including through profiling. They may have legal effects or similarly significantly affect data subjects. These automated decisions are always based on one of the legal grounds provided for in Article 22 of the GDPR, namely: a) authorisation by law; b) entering into and performance of a contract; or c) the data subject's explicit consent.

### **a) Legal authorisation**

We make automated individual decisions based on legal authorisation (including mandatory measures in the public interest) in areas such as customer due diligence, the prevention and combating of money laundering and terrorist financing, and the implementation of international sanctions. For this purpose:

- we check whether you are included in databases of persons accused of financing acts of terrorism or economic crimes, persons at high risk of fraud, or persons subject to international sanctions;
- we use profiling mechanisms and automated decision-making processes to continuously monitor our client portfolio and their transactions for the purposes of preventing and combating money laundering and terrorist financing and implementing international sanctions.

These mechanisms and processes may use data collected about you as part of the customer due diligence process, as well as data from public sources or obtained from data aggregators. They may also use artificial intelligence-based models.

If the individual assessment shows that your profile exceeds the level of risk accepted by the Bank, we may • refuse to enter into a relationship with you; • impose restrictions on the existing relationship; • suspend/refuse transactions; or • unilaterally terminate the relationship.

The use of these automated decision-making processes:

- reduces the risk of human error and discrimination;
- allows banking services to be provided in accordance with the law, without hindering the onboarding and transaction management processes; and
- enables the accurate collection and reporting of information on clients and transactions, in accordance with the law.

## **b) Entering into and performance of the contract**

### **Conclusion of the contract**

For certain banking products, we use automated scoring-based decision-making to enter into a contract with you.

For example, we use credit scoring to assess your eligibility for the credit you have applied for. The algorithms we use for credit scoring take into account various criteria, in accordance with our risk policy, such as: • your financial situation, • creditworthiness, • level of exposure, • payment behaviour, • employment status, • debt history, etc. The criteria and algorithms that we consider relevant may vary over time.

### **Performance of the contract**

We use automated decision-making to ensure the security of the Bank's products and services and to protect you against the risk of fraud. In this way, we ensure the proper performance of the contract with you.

For example, we monitor the payments you make online or by card. If we identify suspicious transactions, we may take automated measures, such as blocking the suspicious transaction, blocking the card, blocking the account, etc. Examples of such suspicious transactions include: • recurring payments that are unusual in terms of frequency or value, • other transactions involving illogical sequences, such as payments made from different locations (cities) within short periods of time that would not allow travel between them using currently available means of transport, • payments that do not match your transactional profile, etc.

### **c) Explicit consent**

If you have given your explicit consent, we may use automated individual decision-making to send you personalised commercial communications (either from us or from BRD Group companies, depending on your choice). For details, please see Chapter III above, including the framework document governing the processing of your data in the Bank–client relationship, available on the BRD website here: <https://www.brd.ro/prelucrarea-datelor-cu-caracter-personal>.

You benefit from appropriate safeguards in relation to all automated decisions we make. In particular, you have the right to:

- express your point of view regarding the automated decision;
- request a reassessment of the decision, through human intervention;
- to challenge the automated decision.

## **V. TO WHOM DO WE DISCLOSE THE PERSONAL DATA?**

We can disclose personal data to:

### **a) Our main service providers, such as:**

- interbank payment processing services and the transmission of information on payment transactions through interbank payment and communication schemes/systems, e.g.: The Society for Worldwide Interbank Financial Telecommunication

(SWIFT), Transfond and the National Bank of Romania (NBR) for the national payment systems ReGIS and SENT;

- Beneficiary Name Display Service (SANB): Transfond and participants in the SANB Scheme. The list of participants is available at:

<https://www.transfond.ro/pdf/Lista%20b%C4%83ncilor%20care%20ofer%C4%83%20SANB.pdf>.

In the context of payment services administered by Transfond: state institutions and authorities with supervisory and control powers, such as the National Bank of Romania (NBR);

- RoPay service: Transfond and participants in the RoPay Scheme. The list of participants is available at: <https://www.transfond.ro/servicii/casa-de-compensare-automata-sent>.

In the context of payment services administered by Transfond, state institutions and authorities with supervisory and control powers, such as the National Bank of Romania (NBR);

- international card organisations (Mastercard, Visa, etc.);
- payment processing services;
- transaction reporting services to competent authorities or other regulated entities (Deutsche Börse, DTCC, etc.);
- bank card issuance and personalisation services;
- debt recovery and debt collection services;
- valuation services for goods and other assets;
- investment agents/brokers in the capital markets.

### **b) Our marketing service providers, such as:**

- marketing agencies;
- market research and analysis agencies;
- marketing communications service providers (e.g. e-mailing of commercial offers);
- partners specialising in organising prize draws and competitions.

### **c) Our support or ancillary service providers, such as:**

- electronic communications services (e.g. e-mailing, SMS, etc.);
- real estate agents;
- enforcement agents;
- IT services (e.g. maintenance, support, development);
- audit services;
- physical and electronic storage and archiving services;
- courier services;
- legal, notarial or other consultancy services.

### **d) Public institutions and authorities in Romania or abroad, such as:**

- National Bank of Romania (NBR);
- Financial Supervision Authority (ASF);
- National Supervisory Authority for Personal Data Processing (ANSDP);
- National Office for the Prevention and Combating of Money Laundering (ONPCSB);
- The Office for the implementation of International sanctions;
- National Agency for Fiscal Administration (ANAF);
- The Competition Council;
- National Archives;
- Courts and other judicial authorities: police authorities, Public Prosecutor's Offices attached to the courts, the National Anticorruption Directorate (DNA), etc.;
- The Bank Deposit Guarantee Fund - FGDB.
- National Credit Guarantee Fund for Small and Medium-Sized Enterprises (FNGCIMM);
- Deutsche Boerse Approved Reporting Mechanism (ARM).
- General Directorate for Personal Records (DGEP).

### **e) Certain clients of the Bank with whom you have contractual relationships or other legal relationships connected with our services, such as:**

- utility service providers (water, electricity, telephone, internet, etc.), in the case of direct debit arrangements;

- companies with which you have employment relationships and which have entered into salary payment arrangements with us.
- f) The **legal representative** of a person lacking legal capacity or having limited legal capacity.
- g) **Other partners of the Bank**, such as:
  - the Credit Bureau (to which we also report data on payment arrears);
  - other financial and banking institutions, for example: • correspondent banks, • other financial and banking entities participating in interbank payment and communication schemes/systems (SEPA, ReGIS, SENT, SWIFT, etc.);
  - the National Public Pension House (where pension benefits are paid into an account held with the Bank);
  - Central Depository;
  - pension and/or insurance companies;
  - insurance brokers/loss adjusters;
  - investment fund management companies (which provide services to the Bank or for which the Bank provides services),
  - other entities (banks, other financial and banking institutions, etc.) in the event of the assignment or restructuring of portfolios of receivables, the assignment of contracts or of the Bank's rights arising from its relationship with you.
- h) **entities within the Société Générale Group and the BRD Group**, such as: Société Générale S.A., Société Générale Global Solution Centre India (SG GSC INDIA), Société Générale Global Solution Centre Romania (SG GSC ROMANIA), in accordance with the law. To view the full structure of these groups, please visit: <https://www.brd.ro/despre-brd/noutati-si-presa/ultimele-noutati> and <https://www.societegenerale.com>.

## VI. DATA TRANSFER ABROAD

As a rule, we transfer personal data only to countries within the European Economic Area (EEA) or to countries recognised by a decision of the European Commission as providing an adequate level of protection.

However, we may also transfer personal data to other countries in the following circumstances:

- a) where the transfer is based on **appropriate safeguards**, such as the use of:
  - standard data protection clauses adopted by the European Commission or another competent authority (where applicable, together with additional safeguards, details of which we can provide upon request);
  - other clauses approved by the competent authority; or
  - binding corporate rules applicable within BRD.
- b) where the transfer is made pursuant to **international treaties** between the European Union and the third country (e.g. agreements between the EU and the US);
- c) where the transfer is **necessary for the performance of the contract** with you. For example, if you wish to transfer funds from your account to an account held with a bank located in a third country, we must disclose your personal data in order to execute the requested banking transaction;  
**Note:** In order to make international funds transfers, the Bank uses the settlement services provided by SWIFT. SWIFT temporarily stores data relating to transactions processed through the SWIFT platform on servers located in the EU and the US. Under applicable law, SWIFT may be required to disclose data stored on servers in the US to US authorities for the purposes of preventing money laundering and combating terrorist financing.
- d) in other cases permitted by law.

We may also transfer your personal data to other entities within the Société Générale Group, as set out in Chapter III (mainly point E) and Chapter V of this Notice.

## VII. WHAT ARE YOUR RIGHTS?

Under the law, you have the following rights in relation to the processing of your personal data by the Bank:

- a) **Right of access:** you may obtain from us confirmation as to whether we process your personal data and information about: • the purposes of the processing, • the categories of data processed, • the recipients of the data, • the data retention period, • your right to rectification, erasure or restriction of processing.  
 You have the right to obtain a copy of the personal data undergoing processing free of charge, and additional copies for a fee.
- b) **Right to rectification:** you may request the correction of inaccurate personal data concerning you and the completion of incomplete personal data.
- c) **Right to erasure:** you may request the erasure of your personal data where: (i) they are no longer necessary for the purposes for which they were collected; (ii) you have withdrawn your consent to their processing and we can no longer process them on any other legal grounds; (iii) the data are processed unlawfully; or (iv) the data must be erased in accordance with the law.
- d) **Withdrawal of consent:** you may withdraw at any time the consent you have given to the processing of personal data based on your consent. This does not affect any processing carried out prior to the withdrawal of your consent.
- e) **Right to object:** you may object at any time to processing for marketing purposes (including profiling carried out for such purposes) and, on grounds relating to your particular situation, to processing based on BRD's legitimate interests.
- f) **Restriction:** you may request the restriction of the processing of your personal data in the following circumstances:
  - (i) when you contest the accuracy of such data (for the period during which we verify their accuracy);
  - (ii) where the processing is unlawful and you do not want the data to be erased, but instead request the restriction of their use;
  - (iii) where we no longer need the data for processing purposes, but you require them for the establishment, exercise or defence of legal claims; or
  - (iv) where you have objected to the processing (for the period during which we verify whether our legitimate grounds for processing override your rights as a data subject).
- g) **Right to data portability:** you may request that we, in accordance with the law:
  - receive the personal data you have previously provided to us in a structured, commonly used and machine-readable format (e.g. CSV format); and
  - have these data transmitted to another entity, where technically feasible.

You have this right to data portability only where both of the following conditions are met: (i) the processing is carried out by automated means; and (ii) the processing is based on your consent or is necessary for the performance of a contract with you.

- h) **Rights relating to our automated decision-making:** for details, please see Chapter IV of this Notice.
- i) **Right to file a complaint with the National Supervisory Authority for Personal Data Processing:** you have the right to file a complaint with this authority if you consider that your rights have been infringed. Its contact details are as follows:  
**National Supervisory Authority for Personal Data Processing**  
 Mailing address: Blvd. G-ral. Gheorghe Magheru 28-30 Sector 1, postal code 010336, Bucharest, Romania  
 E-mail: [anspdc@dataprotection.ro](mailto:anspdc@dataprotection.ro)

To exercise the rights mentioned in letters **a) - h)** above, you can contact us at the contact details mentioned in chapter VIII below.

The following rights also apply to the Client's authorised representatives and legal representatives: • the right of access, • the

right to rectification, • the right to erasure, • the right to restriction of processing, • the right to object, and • the right to lodge a complaint with the National Supervisory Authority for Personal Data Processing.

## **VIII. CONTACT**

If you have any questions about this Notice or wish to exercise your rights as a data subject, you may contact us using the following contact details:

**BRD-Groupe Société Générale S.A.**

**For the attention of: BRD Data Protection Officer (DPO)**

**Mailing address: Blvd. Ion Mihalache, no. 1-7, sector 1, BRD Tower, postal code 011171, Bucharest, Romania**

**E-mail: [dataprotection@brd.ro](mailto:dataprotection@brd.ro)**

## **IX. FINAL PROVISIONS**

In clients are represented by other persons in their relationship with the Bank, their authorised representatives/legal representatives shall inform the clients they represent about:

- the existence and content of this Notice regarding the processing of personal data and
- the fact that this document is available free of charge at BRD branches and on the Bank's website, in the section <https://www.brd.ro/prelucrarea-datelor-cu-caracter-personal>.

Regarding the processing of personal data in the context of entering into a business relationship with the Bank and updating your data, this Notice is supplemented by the specific notice concerning the cooperation with the General Directorate for Persons Records, available on the Bank's website in the following section: <https://www.brd.ro/colaborare-brd-evidenta-populatiei>.