

GENERAL BANKING TERMS for INDIVIDUALS

July 4th, 2022

GENERAL ISSUES ON ACCOUNTS	1	A) Notion	19
I. Introduction	1	B) Type of Deposits	19
A) Preamble	1	C) Features	19
B) Interpretation	2	IV. Other Savings and Investment Products	20
C) Scope	7	V. Savings Accounts (Atustart, Atusprint, Atucont, Smart Cont)	20
II. Opening, Operation and Closing of Accounts	7	A) Notion	20
A) General	7	B) Types of Savings Accounts	20
B) Opening of Accounts. Account Proxy	8	C) Features	20
C) Account Operation and Performance of Payment Transactions	8	D) Allowed Transactions	20
D) Proof of Transactions and Statement of Account	12	E) Rights and Obligations of the Client	20
E) Closing of Accounts	13	F) Rights and Obligations of the Bank	21
III. Rights and Obligations of the Parties	14	VI. Bank Card	21
A) Rights of the Client	14	A) General	21
B) Obligations of the Client	14	B) Conditions for use of cards	22
C) Rights of the Bank	15	C) Savings derived from using cards at POS	28
D) Obligations of the Bank	16	VII. Insurances	28
IV. Know Your Client, Prevention of Money Laundering and Terrorism Financing	16	VIII. Granting of Loans/Overdrafts, Guarantees	28
V. Confidentiality	17	IX. The Safe Deposit Box	29
VI. Final Provisions	17	X. Remote Banking	32
A) Amendment of the Contract	17	A) General Principles	32
B) Duration of the Contract	17	B) MyBRD Contact Service	34
C) Client – Bank Communication	17	C) MyBRD SMS Service	35
D) Guarantee of Funds Held	18	D) MyBRD Net Internet banking Service	36
E) Force Majeure	18	E) MyBRD Mobile banking Service	39
F) Applicable Law. Disputes	18	XI. Changing/ Switching Accounts Service	42
G) Other Provisions	19	PACKAGES OF PRODUCTS AND SERVICES	43
BANKING PRODUCTS AND SERVICES	19	I. General Principles	43
I. Nominal Current Account	19	II. Purchasing a package of Products and Services	44
II. Revolving Account	19	III. Fees	44
III. Term Deposits	19	IV. Changing of the Structure of Packages of Products and Services	44
		V. Changing the Package Held with Another One	44
		VI. Terminating the Package of Products and Services	44
		VII. Closure of the Products and Services within the Package	45
		ANNEX	46
		Information note on the processing of personal data	46

GENERAL ISSUES ON ACCOUNTS

I. INTRODUCTION

A. PREAMBLE

The relations between BRD - Groupe Société Générale SA and its retail Clients are governed by these General Banking Terms, the provisions of the forms specific to each product or service, the

Bank's normative documents, legal provisions and internal regulations in force, the regulations of the National Bank of Romania, as well as the usages and practices of domestic and international banking. These relations are based on mutual trust, confidentiality and good faith.

BRD - Groupe Société Générale is identified with the following:

- Address: 1-7 Ion Mihalache Blvd., Sector 1, Bucharest, Romania
- Tel: +4021.301.61.00; Fax: +4021.301.66.36;
<http://www.brd.ro>

- Tax Identification Number 361579, registered with the Trade Register under no. J 40/608/1991
- Registered in the Register of Credit Institutions under number RB-PJR-40-007/18.02.1999
- Code of registration for VAT purposes: RO 361579
- NSC Certificate no. 255/06.08.2008 registered with the Public Register of the NSC under no. PJR01INCR/400008

B. INTERPRETATION

B.1 In this document, the following terms shall be interpreted as follows:

- 1. 3D Secure** - security protocol for online transactions performed with the card on the websites that are enrolled in this service and displays the logos: "Verified by Visa" or "MasterCard Secure Code".
- 2. Acquirer:** means any:
 - Entity (public institution or person, irrespective of the legal form of organization, authorized by law to do business) that has a contract to accept Cards with a commercial bank or
 - Unit of a commercial bank or automatic teller machine that enables Card transactions.
- 3. ANAF:** National Agency for Fiscal Administration, the competent authority of Romania for CRS.
- 4. Stateless person:** the foreigner who does not have citizenship of any state.
- 5. Apple Pay** is a digital wallet type application offered by Apple Distribution International, whereby the Client can register the eligible cards issued by BRD - Groupe Société Générale S.A. to perform transactions using the Apple devices compatible with this application.
- 6. Authentication:** the procedure allowing the Bank to verify the identity of a Client or the validity of the use of a Payment Instrument, including its customized Security elements.
- 7. Strict authentication of the Client:** Authentication based on using at least two of the following elements: knowledge, possession, inherence and which are independent of each other and are designed so as to protect the authentication data confidentiality.
- 8. Authorization of a Payment Operation:** the procedure whereby the paying Client's consent for a payment operation is expressed in order to make the Payment Transaction. The consent for a Payment Transaction may be expressed differently by the Client depending on the Payment Instrument used for ordering that Operation. The consent may be expressed by:
 - Signature for Payment Transactions arranged on paper or on the specific Forms/contracts;
 - For Remote Banking Services: the use of the customized Security Features;
 - For cards: the use of the customised Security features and according to Section VI Bank Card, **chapter 4. Authorization and performance of Payment operations.**
 In the absence of a consent expressed in the ways mentioned above, the Payment Transaction is considered unauthorized.
- 9. Authorization to change the payment account (or "Authorization"):** the form by which the Account Holder asks the previous Payment Service Provider and the recipient Payment Service Provider to perform transactions related to the change of account.
- 10. Bank:** BRD - Groupe Société Générale, and any reference to the Bank in the content of the Contract shall be understood as including any of its territorial units (working point, agency, branch).
- 11. Beneficial owner:** means any individual who ultimately owns or controls the Client and/or the individual on behalf or in the

interest of whom a Transaction, an operation or an activity is made directly or indirectly.

12. Card: electronic payment instrument through which the Holder/User has access to the money in the attached Account, opened in the same currency with the Bank, in compliance with the Contract.

By filling in the standard forms of the Bank, the individual requests the opening of a Current Account in his/her own name/requests the attaching to an existing Current Account of a Debit Card usable on that Account, thus becoming the holder of an account with an attached Debit Card.

By filling in the standard forms of the Bank and following an analysis of the creditworthiness, the Client may become the Holder of a Credit Card.

13. Payment Incidents Register - a structure within the NBR specialising in managing specific information of payment incidents caused by account holders with cheques, bills of exchange and promissory notes, for public interest, including for the users' specific purposes.

14. Central Credit Register - the structure within the NBR specialized in managing credit risk information and card fraud information, for the specific purposes of the users, while maintaining the professional secrecy.

15. Client: any individual with whom the Bank, in consideration of the activities permitted by the banking law, has negotiated a transaction, even if such transaction has not been completed, and any individual who receives or has received the products/services of the Bank, including the Account Proxy.

16. Beneficiary Client of the payment: the Client intended as the recipient of the funds which have been the subject of a Payment Transaction.

17. Paying Client: a Client making a payment in the Current Account, as the holder/Account proxy/legal representative.

18. Vulnerable client from a financial point of view: client with monthly income below the equivalent of 60% of the gross medium salary/economy projected in the last macroeconomic forecast, the autumn forecast, published by the National Committee of Prognoses, in the current year for the next year or whose income in the last 6 months does not exceed the equivalent of 60% of the gross medium salary/economy.

19. BIC code (Bank Identifier Code): a code that is specific and unique to each individual Bank and represents the method of identifying banks in the S.W.I.F.T. system (Society for Worldwide Interbank Financial Telecommunication). The BIC code of BRD is BRDEROBU.

20. Unique identification code: IBAN or any other code needed to identify the payee.

21. International telephone/fax code: the code of the country of origin of the telephone/fax operator (e.g. ROU – Romania).

22. Current Account: the basic element in the relationship with the Client, which is the support product for various banking services and products, utilised for execution of payment operations.

Any reference to the "current account" shall be considered as being made including "payment account with basic services"

23. Payment account accessible online - payment account that can be accessed by the payment service user through an online interface.

24. Basic payment account or current account with basic payment services: payment account offering the following types of services:

- (a) services enabling all the operations necessary for the opening, administration and closing of a payment account;
- (b) services that allow the deposit of funds in a payment account;

(c) cash withdrawal services within the European Union, from an account over the counter or at ATM, during or outside the working hours of the credit institution;

(d) making the following payment transactions within the Union: (i) direct debits; (ii) payment transactions through a payment card, including online payments; (iii) credit transfers, including standing orders, as appropriate, to bank terminals, counters and through the credit institution's online facilities.

The payment account (current account) with basic services is available in Lei.

The payment account (current account) with basic services is offered to Clients who do not have, at their request, another payment account, including a basic payment account, at a credit institution in Romania, unless the Client declares to have been notified of the closure of the account.

The fees applied for a current account with basic payment services differ depending on whether the client is in the "vulnerable clients from financial point of view" sphere.

25. Revolving Account: an account opened by the Bank providing the Client access to cash provided by the Bank in the form of credit lines, only through a credit card. This account reflects all the transactions made via the credit card, and the fees, interest and premium related thereto.

26. Technical account: an account assigned to the Client, opened and used exclusively by the Bank for technical management needs in connection with (i) the establishment of disposals (e.g. garnishments, measures of unavailability, etc.) and (ii) certain operations performed by the Client or requested by, but not limited to: crediting the Accounts, extending the maturity of a payment obligation, cashing the insurance premiums or the amounts of money to which the Bank is entitled.

27. Contract: these General Banking Terms, which are the general framework for the Client-Bank relationship, with the specific forms and contracts concluded by the Client for each product or service, and the Guide of fees and commissions for Individuals and the List of interests in force upon recording the Client in the Bank's records.

28. CRS (Common Reporting Standard): regulation of the Fiscal Procedure Code on administrative cooperation procedures in the field of taxation, which establishes the obligation of the Bank to collect and report to ANAF, CRS Information on Client account holder.

CRS Information: data and information on the fiscal status of the Client account holder, as regulated by the Fiscal Procedure Code.

29. Exchange rate: the exchange rate used as a basis for the calculation of the foreign exchange provided by the Bank or coming from a public source.

30. Exchange rate applicable to card related transactions: the exchange rate applied to Card transactions when the currency of the Current/Revolving Account differs from the currency of the transaction or the settlement currency of card organizations, if applicable. Details of the method of calculation and the exchange rate applied to transactions made with the card are available on www.brd.ro.

31. Foreign currency date: the reference date used by the Bank to calculate the interest on the amount debited or credited in the Account.

32. Direct debit: national or border payment service for debiting of the payment account of paying Client, when a payment operation is initiated by the Beneficiary of the payment based on paying Client's consent.

33. Unauthorized overdraft: the debit balance recorded in the Current Account or the balance exceeding the value of the credit line granted for the Current Account or the Revolving Account, resulting from the payment operations made from the account and/or from the non-payment of the interests, charges and/or other amounts owed by the Customer. Unauthorized overdraft is a payment obligation with immediate maturity, from the time of its recording in the account.

34. Holder: an individual, the Account holder holding a Card issued by the Bank.

35. Customized Security Features: vary depending on the type of product/service.

For Cards:

- CVC2 (Card Verification Code) and CVV2 (Card Verification Value) is a three-digit code, written on the back of the Card, which can be used to perform transactions over the Internet or by mail order, telephone, fax or for enrolling a Card in a digital wallet type application/service Apple Pay or Google Pay type etc. (enabling the Users/Holders of Cards enrolled in an application installed on certain devices compatible with the NFC Technology (such as smartphones, smartwatches, smart bracelets, etc.), to perform transactions with the help of such devices). This code should remain known only by the holder/user of the Card;

- e-Commerce Password: composed of the static password, defined by the Card User/Holder on the transaction's authentication page and of a dynamically generated unique code for each online transaction performed on the 3D Secure websites holding the service "Visa Secure" or "MasterCard Identity Check". The 3D Secure code is sent to the Card User/Holder via SMS on the phone number declared by the User to the Bank and required for validating the transactions with vendors enrolled in the 3D Secure system. The 3D Secure code is issued for each online transaction on a 3D Secure enrolled website, being unique/operation and valid for 15 minutes. The Bank reserves the right to refuse the approval of transactions unaccompanied by the e-Commerce Password.

This method of authorizing online transactions shall be applied only as an exception, only to the Card User/Holder that doesn't have the BRD Mobile banking application.

- the PIN code of the device where the digital wallet type application/service is installed;

- token PIN (mPIN) – the numeric password consisting of 6 characters, defined by the Client when first accessing the Mobile Banking service.

The biometric authentication represents the cardholder/user authentication through the Mobile Banking BRD application, through biometric data (such as but without being limited to Touch ID, Face ID), to authorize card transactions performed with the cards enrolled in the digital wallet type service and card transactions over the Internet, according to the applicable regulations;

- Face ID (facial recognition): method of identification of the owner of the device based on the authentication secured by advanced technologies, enabling the accurate mapping of the facial geometry by the used device.

- Touch ID (digital fingerprint): fingerprint data enabling the unique identification of the individual it belongs to, as it was recorded on the used mobile device (smartphone/tablet).

- the activation code is a unique verification code sent to the Card holder via SMS, over the mobile phone number of the Holder/User declared to the Bank, in order to validate the capacity of Card owner desiring to enrol in a digital wallet type application/service;

- PIN – a personal identification code provided by the Bank for Card Transactions in electronic payment terminals and ATMs. The PIN number is strictly personal and confidential and should not be revealed to anyone, under any circumstances, regardless of the context.

For Remote Banking Services - Security Codes:

- User ID and Password to access MyBRD Net Internet banking service, MyBRD Mobile tablet banking service accessed through mobile web browser and MyBRD Contact;

- PIN number for MyBRD SMS and MyBRD Mobile accessed via USSD session;

- Token PIN (mPIN)/ digital fingerprint for MyBRD Mobile tablet banking service accessed through the dedicated smartphone/tablet application or hardware/mobile token for MyBRD Net Internet banking service;

- Biometric authentication.

36. FATCA – the acronym of the US law called the “Foreign Account Tax Compliance Act” and represents a set of regulatory measures adopted in March 2010 by the Senate of the United States of America (USA) in order to prevent and reduce the tax invasion generated by the cross-border activity of US residents, which requires reporting by the foreign financial institutions (registered in a country other than USA) of US citizens, including those living outside the US borders, to the US Tax Authorities (IRS – Internal Revenue Service). FATCA was implemented in the national regulatory framework by Law no. 233/2015 regarding the ratification of the Agreement between Romania and the United States of America for the improvement of international tax compliance and for the implementation of FATCA.

37.1. FATCA non-compliant client: the person who refuses to submit the required document to clarify the U.S. Person status thereof or refuses to agree to report under FATCA requirements or has not answered the request for information by the set deadline although U.S. indicia have been identified, they have not been updated or confirmed. Starting from 1 July 2014, the Bank does not accept starting a relationship with any new FATCA non-compliant client.

37.2. Affidavit (FATCA) is the statement made by the Bank Client/contractual partner whereby the same confirms the status determined by the FATCA regulation.

37.3. USA person (or American person): any individual regulated by USA laws, obliged to pay taxes in the USA. People in the USA are American taxpayers whether they live in the USA or outside the USA territory. The indications that an individual may be considered a “USA Person” are as follows: (i) the client is a USA citizen; (ii) the client is a USA resident (Green Card holder); (iii) the client has a USA address (main address/ mailing address); (iv) the client's place of birth is in the USA ; (v) the client's current telephone number is from the USA; (vi) the client has set up a scheduled payment order from a BRD account to a USA account; (vii) there is a proxy or power of signature on the client's account, currently valid, granted to a person with a USA address (account proxy given to a person with a USA address).

38. Google Pay is a digital wallet type service provided by Google, whereby the Client can register Cards issued by BRD - Groupe Société Générale S.A for carrying out transactions with Android devices compatible with this service.

39. BRD Group: BRD – Groupe Société Générale S.A, together with subsidiaries and affiliate companies.

40. The Groupe Société Générale - a banking group carrying out organized activities at international level, of which the Bank is a part. To see the complete structure of the BRD Group and Société Générale, please visit: <https://www.brd.ro/despre-brd/noutati-si-presa/ultimele-noutati>.

41. IBAN (International Bank Account Number) means a combination of letters and figures which provide a unique number of an account opened with a worldwide payment service provider. The IBAN is provided to the Client by the Bank on the date of account opening and is also referred to in each account statement.

41. Credit institutions involved in carrying out transfers of funds abroad: (i) the authorizing bank, the one to which the authorizing officer gives disposition regarding the payment, (ii) the beneficiary bank, the one that receives the payment according to the payment instructions, (iii) the correspondent bank , the one that has direct access to the international interbank network and that mediates the international transfers of funds that another bank cannot make directly, (iv) the intermediary bank, the one that is involved in

making a transfer of funds, other than the ordering bank and correspondent bank.

42. Debit instrument: cheque, bill of exchange or promissory note.

43. Payment instrument: any customized device and/or any set of procedures agreed between the Client and the Bank and used by the Client to initiate a Payment Order (e.g. bank card, Remote Banking Services).

44. Account Proxy: an individual authorized to represent the Client who is the Account holder in the relation with the Bank, appointed by the Client upon opening the account or thereafter, through the Bank forms used specifically for the appointment of the Account proxy or through a genuine mandate expressly granted.

45. Senior Public Official: an individual holding a specific position that does not fall into the category of positions held by PEP (publicly exposed persons), but who is exposed to a significant extent to the risk of corruption and money laundering, and in connection with whom the Bank applies additional know-your-customer measures. According to the internal requirements of the Group to which the Bank belongs, the following people are Senior Public Officials (non-restrictive list):

- the President's Adviser;

- State Counsellors;

- Prefects;

- Deputies of the commander of the armed forces; Deputy Inspector General of the Inspector General; First Deputy and Chief of Staff;

- the Director of the Romanian Intelligence Service, the Director of the Foreign Intelligence Service, the Director of the Special Telecommunications Service; the Director of the Protection and Guard Service;

- Members of the Financial Supervisory Board (President, First Vice President, Vice President); Members of the Competition Council (President, Vice President); the management of the National Fiscal Administration Agency (President, Vice President, Secretary General);

- Governor of the Danube Delta Biosphere Administration (ARBDD);

- Patriarch; Metropolitan; Apostolic Nuncio; Metropolitan Archbishop; President; Vice President; General secretary; Treasurer; Archbishop; Bishop; Mufti;

- Mayor;

- President of the County Council;

- CIO/FIFA/FIBA officials (CIO Steering Committee members; FIFA Board members; FIBA Committee members, etc.);

- Chief Prosecutor of the General Prosecutor's Office, Chief Prosecutor of the National Anti-Corruption Directorate; Chief Prosecutor of the Directorate for the Investigation of Organized Crime and Terrorism;

- Consul General; Career Consul;

- Senior officials of UNESCO, OECD, OSCE, IMF, World Bank, European Central Bank, EBRD, etc.

46. Card usage limits: limits set by the Bank or cards organizations or the European banking authorities for the security of the transactions and the protection of the Holder/User and which refer to both the number and the value of the Transactions that can be performed with the Card within a certain period, available for card users (i) by displaying at the Bank's units (ii) on the Bank's website, (iii) through the Internet banking service MyBRD Net, if it owns this service (available 24 hours a day, 7 days a week), (iv) by calling MyBRD Contact: 021 302 61 61 (regular number in any network) or * BANK (* 22622) (charged as a network call from any Orange, Vodafone, Telekom Mobile and RCS Digi Mobile number).

45. TIN – Tax Identification Number (or functional equivalent if there is no tax identification number) assigned by the tax authorities of Romania / Other countries of residence.

46. Operations that seem to be connected: represent operations whose value is fragmented in smaller tranches and which have common elements such as: transaction parties, including the beneficial owners, the nature or category where the transactions fall and the amounts involved.

47. Payment operation: an action initiated by the paying Client or by the beneficiary of the payment in order to submit, transfer or withdraw funds, irrespective of any subsequent obligations between the paying Client and the beneficiary of the payment.

48. Fee options: In the case of foreign currency payments or for payments in Lei made in favour of the beneficiaries with accounts opened with banks abroad, the Client may choose one of the following options regarding the method of payment of the fees:

“**OUR**” - all the Bank fees related to the payment made through credit transfer are paid by the paying Client (including Bank/intermediary bank charges)

“**BEN**” – all the Bank fees related to the payment made through credit transfer are paid by the Client who is the beneficiary of the funds which have been the subject of a Payment Transaction (including Bank/intermediary Bank fees)

“**SHA**” – the Bank fee is paid by the paying Client and the Bank/intermediary bank fee and the fee of the Beneficiary’s bank are paid by the beneficiary Client.

In the case of foreign currency payments sent to beneficiaries with accounts opened at EU (European Union) / EEA (European Economic Area) banks, the commission option is SHA. The Bank reserves the right to modify the charging option indicated by the Paying Client if it is different from SHA.

49. Payment order: any instruction given by the paying Client to the Bank or by the payee to the Bank requesting the performance of a Payment Transaction.

50. Standing order: an instruction given by a payer to the payments service provider that holds the payment account of the payer to perform the credit transfer at regular intervals or at predetermined dates.

51. Card organization: an international organization (Visa, MasterCard, etc.) governing the terms and conditions of use of own-branded cards.

52. Politically Exposed Persons: individuals who hold or have been held prominent public office. Individuals who exercise under the Law no. 129/2019 prominent public office are:

- heads of state, heads of government, members of government, secretaries of state;
- members of Parliament or similar central legislative bodies;
- members of the governing bodies of political parties;
- members of the Supreme Court, members of the Constitutional Court or other high courts the decisions of whom can only be appealed through extraordinary remedies;
- members of the governing bodies of the courts of accounts or members of the governing bodies of the boards of central banks;
- Ambassadors, *chargés d'affaires*, high-ranking officials from the armed forces;
- Members of Boards of Directors and supervisory boards and persons with management positions in the autonomous administrations, majority State owned trading companies and national companies;
- directors, deputy directors and members of the board of directors or members of the governing bodies of an international organization.

None of the categories mentioned above includes persons holding intermediate or lower positions.

52.1. The family members of the politically exposed person are, according to Law 129/2019:

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

52.2. Persons known to the public as close associates of the individuals exercising prominent public office are, according to Law 129/2019:

- individuals known as the real beneficiaries of a legal person, of an entity without legal personality or of a legal construction similar to them together with any of the persons exposed publicly or as having any other close business relationship with such a person;
- individuals who are the only real beneficiaries of a legal person, of an entity without legal personality or of a legal construction similar to them, known as being established for de facto benefit of one of the person exposed publicly.

53. Foreign payments: Payment Transactions in foreign currency (made abroad or in Romania) and Payment Transactions in Lei performed abroad.

54. Domestic payments: Payment Transactions in Lei, made in Romania.

55. Refusal to pay: the mean by which the Holder/User may challenge an unauthorised Operation or incorrectly executed.

56. Legal representative: an individual who acts as the parent/ caregiver/ legal guardian/ appropriate adult/ special administrator and who has the right and obligation to either conclude civil legal documents for and on behalf of a Client without civil legal competence or to assist a Client with limited legal competence in concluding legal documents and, where applicable, in obtaining the authorisation of the guardianship court to conduct certain transactions.

57. Resident: individual - Romanian citizen, foreign citizen and stateless person residing in Romania, presenting identity documents issued by law.

58. Qualified electronic signature: electronic signature generated by a qualified electronic signature creation device and based on a qualified electronic signature certificate, valid (unrevoked / unsuspended) at the time of signing. According to the specific legislation¹, the qualified electronic signature has the equivalent legal effect of a physical signature. The application of the qualified electronic signature represents the full consent of the Parties and makes its full proof before any court, authority, institution or any other third party.

60. Change/switch of the accounts service: the transfer from one Payment Service Provider to another at the consumer's request, either of information related to all or some of the standing orders for credit transfers, recurrent direct debits and recurring incomings through credit transfers executed in a payment account, either the positive balance of the payment account from one payment account to another, or both, with or without closure of the old payment account.

61. Payment Service Provider making the transfer (Previous Bank) – the payment service provider transferring either the information required to execute the change of accounts or the

¹ The EU Regulation No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/C

possible positive balance of the consumer's payment account or both.

62. Recipient Payment Service Provider (New Bank) - the payment service provider to which the information required to effect the change of accounts is transferred.

63. International sanctions - restrictions and obligations in relation to the governments of some states, with non-state entities or natural or legal persons, adopted by the Security Council of the United Nations, by the European Union, by other international organizations or by unilateral decisions of Romania or other states, for the purpose of maintaining international peace and security, preventing and combating terrorism, ensuring respect for human rights and fundamental freedoms, developing and strengthening democracy and the rule of law and fulfilling other purposes, in accordance with the objectives of the international community, international law and European Union law. International sanctions concern, in particular, the blocking of funds and economic resources, trade restrictions, restrictions on operations with dual-use products and technologies and with military products, travel restrictions, transport and communications restrictions, diplomatic or technical-scientific, cultural or sports sanctions.

64. Foreigner: a person who does not have the Romanian citizenship or the nationality of another Member State of the European Union, or of the European Economic Area, or the citizenship of the Swiss Confederation.

65. Durable medium - any tool that allows the Client to store personally-addressed information in a way that is accessible for future reference for an appropriate period of time for information and which allows the unchanged reproduction of stored information.

66. NFC technology (Near Field Communication) - technology based on a high frequency radio communication standard, which allows devices that have this function to exchange data by simple proximity at a short distance.

67. Terminals: electronic or mechanical devices (e.g. POS, ATM, ROBO, imprinter, internet) that allow the Card Holder/User to perform payment Transactions, cash withdrawals and deposits, and other types of transactions, such as: paying utilities, balance inquiry etc.

68. Terminal with Contactless functionality - a terminal that displays the Contactless symbol, equipped with technology that allows quick transactions by simply approaching the card/other device compatible with the NFC technology (phone, smart watch, smart bracelet) and entering the PIN code and/or signing the transaction receipt, if applicable. The "Contactless" payments refer to fast payments, performed on a Terminal with Contactless functionality.

The transactions that can be performed without entering the PIN and/or signing the corresponding receipt are those with a value lower than the limit set by the card organizations and the European banking authorities. These limits are displayed on the Bank's website and can be changed at any time by the card organizations or European banking authorities.

69. Token is a unique series of numbers in digital format which ensures the secure substitution of the data of a Card registered by the Client in a digital wallet type application/service or enrolled on vendor's websites/applications. The Token number is different from the number on the front of the Card, in order to increase the transaction security.

70. Credit transfer - the national or cross-border payment service to credit of a payee's payment account through a payment transaction or a series of payment transactions made from the payer's payment account by the payment service provider that holds the payer's payment account based on an instruction given by the payer.

Credit transfer includes:

- domestic and external payments;
- domestic and external incomings.

71. Offline transaction: represents the transaction made with a card at a terminal which accepts transactions performed without obtaining an authorisation code from the card issuing Bank and for which the funds are not blocked at the transaction date, but the account is debited with the transaction value at the date, but the account is debited with the transaction value at the settlement date.

72. Country of legal residence: the country where the Client resides. This is evidenced by the submission by the Client of the following documents, mentioning that the Bank has the right to request other additional documents, if necessary, in accordance with the legal provisions and/or internal norms:

- **Romanian citizens residing in Romania:** a) the identity card or b) the identity bulletin or c) the temporary identity card or d) the electronic identity card or e) simple identity card;

- **Romanian citizens residing abroad:** a) the simple electronic passport (CRDS), or b) the simple temporary passport and/or c) the temporary identity card - issued by the Romanian authorities, proving the domicile in a country other than Romania;

- **Foreign citizens with permanent residence in Romania:**

- a) The permanent resident card for citizens of the European Union (EU) Member States, of the European Economic Area (EEA) or Swiss Confederation citizens (CH), with permanent residence right in Romania, issued by the General Inspectorate for Immigration within the Ministry of Internal Affairs (IGI); or
- b) The permanent residency permit in Romania or the long-term residence permit or the residence permit bearing the mention "long-term resident – EC" issued by IGI; or
- c) The permanent resident card for family members of an European Union citizen issued by IGI; or
- d) The permanent resident card for the family member of a Swiss Confederation citizen issued by IGI; or
- e) Identity card or passport issued by Member State of the EU or EEA mentioning the Romanian residence.

- **Foreign citizens – with temporary residence right in Romania:**

- a) The passport or identity card from the country of origin for EU/EEA/CH citizens;
- b) The passport from the country of origin for citizens of third States (non-EU, non-EEA, non-CH);
- c) The registration certificate issued for the citizens of EU Member States or of EEA and for the Swiss Confederation citizens, with residence right in Romania for more than 3 months, issued by the IGI (the General Inspectorate for Immigration), or
- d) Resident card for family members of EU citizens, issued by IGI (the General Inspectorate for Immigration), or
- e) Resident card for family members of Swiss Confederation citizens, issued by IGI (the General Inspectorate for Immigration), or
- f) The temporary residence permit/work permit issued by IGI (the General Inspectorate for Immigration), or
- g) The EU Blue Card - document issued by IGI (the General Inspectorate for Immigration), proving the websites temporary residency in Romania;

- **Stateless persons (without citizenship) and refugees:**

- a) The residency permit in Romania, specifying that the respective person is stateless/without citizenship or a refugee or under subsidiary protection issued by IGI (the General Inspectorate for Immigration), or
- b) Work permit issued by IGI (the General Inspectorate for Immigration), or
- c) The EU Blue Card - document issued by IGI (the General Inspectorate for Immigration), or

- d) Travel document issued based on the Geneva Convention of 28.07.1951

- Employees of diplomatic missions and consular offices:

- a) Diplomatic identity card/special identity card or
b) Diplomatic passport – used when the individual does not yet have the diplomatic identity card.

- Clients who are USA persons:

- a) Identity documents issued by the Romanian authorities for US Persons: residence permit, work permit, certificate of registration, in case the respective client also has EU citizenship, documents issued under the law, as well as
b) Identity documents issued by the US official authorities for US citizens provided they prove the identity, citizenship, domicile/ residence address (e.g. passport and/or driving licence and/or Green Card, etc.).

73. Country of residence for tax purposes: is the country where, in terms of tax an individual is taxed according to the criteria stipulated in the respective country's legislation. The Bank will consider that the country of tax residence of the individual is the one mentioned in the official identity document, the passport or any other proof of identity presented by the individual. Exceptions: if the individual communicates other country of tax residency that the one stated in the official identity document, the passport or any other documentary proof of identity presented, the country of tax residence shall be proved by the individual by submitting a tax residence certificate issued by the tax authority/competent authority under the laws of that country to issue such documents. In the absence of this certificate, the Bank shall consider the country of tax residence, the country that issued the official identity card, passport or other proof of identity. An individual who is not resident in Romania and is resident for tax purposes in a country that has concluded a convention for the avoidance of double taxation with Romania, and who receives income, subject to withholding, including interest paid by the Bank, to benefit of the application of tax conventions providing for withholding an income tax rate lower than that of the Fiscal Code is required under Romanian legislation, to submit to the Bank unit which has opened the account before receiving income, the tax residence certificate, issued by the fiscal authority/competent authority to issue such documents in its residence country tax, in original and accompanied by a certified translation thereof in Romanian language, valid at the interest payment date/ date of registering in the account. In the case of interest income, it is considered the date of cashing income the date of registration of the interest in the account of the individual.

The tax residence certificate submitted in a year in which the Bank conducts interest payment is valid all current year and another 2 months of the following calendar year, if do not contains explicit provisions limiting the validity of a certain period of time.

74. User: an individual with the minimum age of 14, on behalf of whom the issue of a card has been requested (by the standard forms of the Bank and by providing identification data), to whom the Client who is the Account holder has given the right to perform transactions in the Current Account/Revolving Account of the latter as the Account Proxy.

75. Business day: it is a bank day (excluding Saturdays and Sundays and other bank holidays recognized in Romania) when the Bank carries out specific activities and is open to the public.

B.2. In these General Banking Terms, the use of defined terms in the singular implies the plural and vice versa.

B.3. All provision relating to CRS from the present General Banking Condition shall be completed with the provisions from the Fiscal Procedure Code.

C. SCOPE

1. The provisions of the chapter on “General Issues on Accounts” shall be supplemented by the provisions of the Chapter on “Products and Services offered by the Bank” and the provisions of specific contracts, forms for each product/service.

2. The Contract enters into force from the date of signing as proof of acceptance by the Client, with handwritten signature or qualified electronic signature and remains in effect until the closure of all Client accounts and the termination of the effects of all specific contracts concluded with it.

3. These General Banking Terms replace the previous versions of the General Banking Terms.

4. These General Banking Terms replace any contrary provision in the contracts, forms and/or documents specific to the products and services, concluded before the entry into force of the General Banking Terms and, where appropriate, supplement them.

5. In case of conflict between the provisions of these General Banking Terms and the special conditions of contracts, specific documents and/or forms concluded between the Client and the Bank on the same day or after the entry into force of these General Banking Terms, the special conditions of the specific forms or documents shall prevail.

6. The amendment or termination of any of the specific contracts concluded between the Client and the Bank shall be performed under the terms of those contracts and shall not affect the validity of the other contracts or these General Banking Terms.

7. Any waiver of the enforcement of the Contract against the Client shall be specifically agreed in writing between the Bank and the Client.

II. OPENING, OPERATION AND CLOSING OF ACCOUNTS

A. GENERAL

1. Entering into a business relationship with the Bank can take place both through the Bank's network and online, through the institutional website www.brd.ro.

2. The Bank is required to verify the identity of the Client and the beneficial owner before establishing a business relationship or conducting transactions. In addition, the Bank has the obligation to verify and collect CRS and FATCA Information of the Client Account Holder. When the Client/ Client Account Holder does not want to provide all the information above, the Bank will refuse to start a relationship with the Client and, implicitly, to open Accounts.

3. The Bank opens different types of Accounts in RON and/or foreign currency such as: Payments accounts (Current accounts/ current accounts with basic payment services with or without Debit Cards attached, Revolving Accounts with Credit Cards attached), deposit accounts, savings accounts, at the explicit request of the Client. The accounts are opened with the Bank units, online through the institutional website www.brd.ro or via the remote banking services, in compliance with this Contract, based on the filling in and signing by the Client of the standard Bank forms, accompanied by the documents requested by it. For clients entering a relation with the Bank, who are opening Accounts through remote banking services or use remote banking services, the Bank may set out specific eligibility conditions, which will be accordingly communicated, in compliance with the Bank's policy and regulations in force. The basic services accounts, as well as accounts having minor children as account holders, can be opened only through the Bank's territorial units.

4. The Bank has the right to open technical accounts, and mutual rights and obligations, shall not be born by the Parties by opening these technical accounts supplementary to those related to accounts opened by the Client.

5. Various products and/or services may be attached to any Account, when the Client requests it and in compliance with the terms of the Bank.
6. The Client has access to all the information, conditions, rights and obligations of the Parties mentioned in the Contract 15 days before the signing thereof, except the case where he/she requests the reduction of such period.
7. At any time during the contractual relationship, the Client is entitled to receive, upon request, the terms specified in this Contract on paper or on another durable medium.
8. The Bank grants access to payment initiation services providers and information providers in relation to the Accounts held by the client, on an objective, non-discriminatory and proportional basis.
9. The Client is entitled to use the payment initiation services supplied by a payment initiation services provider and/or information services provider in relation to accounts supplied by an information services provider. In order to perform these operations, the payment account must be accessible online. The terms are found in chapter X. Remote banking.
10. For establishing products and/or services requiring the availability of amounts in the account according to this Contract/specific contract documentation, the Client undertakes to ensure the availability of this amount on the date of contracting these products/services. If, at the end of the day when those products/services were contracted, the required amounts are not available in the account, such products shall be automatically cancelled due to lack of funds. If the Client has outstanding payment obligations towards the Bank, he/she understands and agrees that first such payment obligations shall be offset, subsequently followed by the establishment of products and/or services requiring the availability of amounts in the account, in the case such amounts are available. The Bank reserves the right not to establish such products/services in the absence of the available amounts.

B. OPENING OF ACCOUNTS. THE ACCOUNT PROXY

1. Upon the Account opening, and, if the case, at the moment of appointing the account proxies, the Bank requires the documents required to identify the Account holder and, if the case, the Account Proxy and their signature specimen for each Account. The appointment of an Account proxy shall not take effect until all the documents necessary for its identification and the signature specimen are submitted by the Account Proxy. In addition, the Client Account holder has the obligation to present to the Bank all CRS Information according to the law in force.
2. If the Client has opted for the changing/switching account service for current accounts, the Bank, as the new bank, will proceed with the Current Account opening/account relationships only after the Client has filled in and signed the Authorization form and the Contract/documents specific to the Bank.
3. The Account Proxy may be appointed by the Account holder through the Account opening contract/ application, through a separate form for appointing/ revoking of Account Proxies made available by the Bank or through the application of issue/increase of the Credit Line (for Account Proxies of Revolving Accounts with an attached Credit Card). In the case of accounts opened online or via the remote banking services, the Bank may restrict the appointment of an Account proxy when opening the account, the Client having the possibility to subsequently present himself/herself to one of the Bank units for appointing a Proxy for these Accounts. The Account Proxy shall always act only for and on behalf of the Client who is the Account Holder.
4. The Account Proxy appointed through the Bank forms has the following rights:
 - a. To perform transactions in the accounts for which he is appointed as Account Proxy, including by means of electronic payment

- instruments provided by the Bank - cards, payment instruments with remote access such as internet banking/mobile banking, etc., unless otherwise provided in the product-specific documentation;
- b. To establish deposits from the Current Account, but only on behalf of the Client who is the Account Holder; on such established deposits only the person/persons which have the capacity of Proxy on the current account will be also Proxy for deposits.
- c. To liquidate the deposits of the Client who is the Account holder as established via that Current Account only if the same is appointed as the Proxy for those deposits.
- d. To request the issuance of the statement of account for the periods when he/she acts as an Account Proxy. The statement of account supplied to the Proxy shall include all operations performed in the Account during that period.
5. When establishing a deposit by the Account holder, he/she is entitled to name account proxies on the respective deposit. Any deposit account Proxy shall also act as a Proxy for the Current Account attached to the deposit. If applicable for establishing deposits with Proxies other than those appointed by the Client who is the Account holder for the Current Account, a separate Current Account shall be opened with different Account Proxies or without Proxies, depending on the request of the Client who is the Account holder.
6. The Account Proxy appointed through the Bank forms may not perform the following:
 - a. Closing/opening new Current Accounts on behalf of the Client who is the Account holder;
 - b. Applying for loans on behalf of the Client who is the Account holder;
 - c. Appointing/revoking other Account Proxies for the accounts of the Client who is the Account holder.
 - d. Liquidating deposits established from a Current Account which do not have a Proxy appointed by the Client who is the Account holder.

These transactions may be performed for the Client who is the Account holder only under an authenticated power of attorney specifically granted in this regard.

7. Any power of attorney granted by the Client Account holder via the Bank forms is considered given for a period of 15 years, with the possibility of revocation at any time. The Client undertakes to inform the agent about the tenure and rights conferred upon the latter by the power of attorney.
8. Empowering a person to represent the Client in relation to the Bank remains valid until the receipt by the Bank from the Client of a written notice or verbal (via MyBRD Contact service) of the revocation, amendment by the Client, waiver by the Proxy with prior notification of the Client or until the Client's death. The termination of the power of attorney becomes enforceable against the Bank from the date of notification of the Bank by presenting a Death Certificate or a written or verbal notice in any Bank units. The Bank is entitled to request any documents considered necessary in relation to these changes.
9. The Client is liable to the Bank for any loss suffered by it as a result of the failure to notify the Bank of any restrictions or limitations regarding the Account Proxy.
10. If a dispute or a conflict of any kind occurs, regarding the appointment, limits or revocation of the power of attorney granted to the Account proxy, the Bank has the right to block the access of the Account Proxy to the account of the Client who is the Account holder up to the dispute settlement evidenced by documents satisfactory to the Bank.

C. OPERATION OF ACCOUNTS AND PAYMENT TRANSACTIONS

C.1 GENERAL ISSUES ON PAYMENT TRANSACTIONS

1. Any operation (e.g. intra/inter-bank payments/transfers in Lei and foreign currency, payment of bills, foreign exchange, receipts, cash deposits and withdrawals, etc.) ordered by the Client/Account Proxy shall be made via the Current Account.

In the payment transactions, the Client shall use the forms and Payment Instruments made available by the Bank.

2. The Revolving Account only works with an attached Credit Card. Lending transactions are allowed for the account (replenishing) by any means: cash deposit, credit transfers from a Current Account for payments opened with BRD or with another financial institution. Any Revolving Account debiting is possible only by using the Credit Card, except for those expressly mentioned in the contract for providing the credit card.

3. The Bank establishes the banking route through which it executes the Payment Operation through transfer credit, including the use of correspondent relationships

4. In the case of inter-bank receipts made by credit transfer in foreign currency, the currency for crediting the beneficiary Client's account will be the one mentioned in the Payment Instruction. If the currency does not correspond to the currency of the beneficiary Account, the Bank will convert the amount into the currency of the Account to be credited, based on the Exchange rate used by the Bank on the day of the transaction and communicated to the Client through the statement of account.

In case of interbank receipts made by credit transfer in Lei, the currency mentioned in the Payment Instruction must correspond to the currency of the Beneficiary Client's account, otherwise the Instruction will not be accepted by the Bank.

In case of intra-bank receipts made by credit transfer in foreign currency, the currency mentioned in the Payment Instruction must correspond to the currency of the beneficiary Client's account and the currency of the debited account, otherwise the Instruction shall not be accepted by the Bank.

The credited account will always be the one indicated in the Payment Instruction.

In case of receipts made by credit transfer in foreign currency that cannot be processed due to the breach of national or international regulations, the Bank shall not be held responsible for the delay of their receipt.

5. For any amount received in the Account, the Bank reserves the right to deduct the fee thereof before crediting it in the Client's account. In this case, the Client shall be informed of the total amount of the Payment Transaction and the fee applied through the statement of account.

6. In the case of inter-bank payments made by credit transfer in foreign currency, the currency for debiting the beneficiary Client's account will be the one mentioned in the Payment Instruction. If the currency does not correspond to the currency of the debited Account, the Bank will convert the amount into the currency of the Account to be debited, based on the Exchange rate used by the Bank on the day of the transaction and communicated to the Client through the statement of account.

7. Before making the payment, the Bank has the right to request the submission of documents allowing the verification of the purpose of the payment, in accordance with legal regulations in force.

8. If the Client requests the cash withdrawal from the foreign currency account of amounts lower than 5 EUR/USD/another currency, they will be exchanged in RON at the exchange rate of the Bank of that day and issued to the Client in that currency.

9. In case of error from the Bank recorded in the Client's Account, the Client specifically authorizes the Bank to correct, at its own initiative, without the prior consent of the Client, the amounts recorded incorrectly.

10. The Bank may set limits/thresholds related to payments for different Payment Instruments.

11. Payment transactions carried out through Debit Instruments shall be made in accordance with the legislation applicable to cheques, bills of exchange and promissory notes and that regarding the Payment Incidents Register.

Payment transactions carried out through debit instruments, available in the Bank's offer, are mentioned in the Guide of fees and commissions for Individuals.

Upon issuing Debt Instruments, the Client shall provide in the Account the available funds required for paying them at the time of issue (in case of a cheque) or on the due date (in the case of bills of exchange and promissory notes), respectively.

12. The Bank is entitled, in case of an Unauthorized Overdraft, to calculate, from the date of its registration in the Account, a penalty interest on the outstanding balance of the Current Account or the Revolving Account, according to the Guide of fees and commissions for Individuals.

13. Any request by the Client for foreign exchange, materialized by signing a foreign exchange order or a contract specific for this type of transaction either settled immediately, or with another currency date, is irrevocable.

14. All the costs arising from the exchange rate differences shall be borne by the Client. Also, both in case of non-compliance with the Order given, and in case of amendment by the Client of the Order sent to the Bank, all the consequences, including but not limited to damages, additional costs incurred by the Bank, shall be borne by the Client.

15. In case of challenging the Transactions performed under a specific contract, the complaint term is the one provided for in the specific contract concluded with the Bank.

16. The Client authorizes the Bank, expressly, without being an obligation, to debit any amounts due under the Contract from any account opened with the Bank (e.g.: current, savings or deposit, etc.). In the case of automatic renewal deposits, the amounts due under the Contract will be debited at the maturity of the deposits, which are subsequently rebuilt with the amount resulting from the debit. The Client authorizes the Bank to perform any foreign exchange operations in order to recover outstanding payment obligations in the currency in which they are to be paid using the exchange rate practiced by the Bank on the day of the foreign exchange transaction. Pursuant to art. 2030 of the Civil Code, the mandate hereby granted to the Bank does not cease in case of the Client's decease, insofar as it applies for performing successive actions within a continuous ongoing activity (e.g. charging the monthly amounts to be paid in relation with loans), in compliance with the right of revocation or waiver of parties or of their successors.

C.2 PRICE

1. The price consists, if applicable, of the following components: fees, interest rates, exchange rates, rates.

2. The amounts of the fees, interest, rates charged by the Bank are found in the Guide of fees and commissions for Individuals and in the List of interests, respectively.

The Client has the possibility to consult, in any moment, the fee information document. The document is available in electronic format on www.brd.ro website, and in any BRD branch on paper or another durable medium.

3. The exchange rates applied by the Bank are shown in the BRD units and on the website of the Bank, www.brd.ro.

4. The Client expressly agrees to the immediate application of any changes of interest rates and exchange rates, without prior notice, if these changes are based on the reference interest rate or the reference exchange rate.

5. Also, any change of interest rates and exchange rates shall be applied immediately, without prior notice, if the change is for the benefit of the Client.

6. The Client shall be informed of these changes as soon as possible by posting in the Bank units and via the Bank's website.

C.3 INFORMATION REQUIRED FOR PERFORMING PAYMENT ORDERS OF TRANSFER CREDIT TYPE

1. For the proper performance by the Bank of a Payment Order of transfer credit type, if the Client is a paying Client, the latter has the obligation to fill in the Payment Orders with the following information:

1.1 Credit transfer type domestic payments:

- The name and account number of the paying Client (IBAN account opened with the Bank);
 - The name and unique identification code of the beneficiary Client;
 - Payment amount;
 - The date of issue of the Payment Order (day, month, year), which should be unique, possible and certain;
- In addition to the information mentioned above, in case of payments made to the State Treasury, the Client shall fill in the following mandatory elements:
- The tax identification code of the paying Client, and of the beneficiary Client, respectively;
 - The payment record number assigned by the National Agency for Fiscal Administration;
 - The number of the Payment Order given by the paying Client;
 - References on the economic content of the Operation.

1.2 Credit transfer type external payments:

- The name of the paying Client;
- IBAN code of the paying Client;
- Payment amount;
- The ordered currency;
- Name of the beneficiary and its full address for payments outside the EEA (European Economic Area);
- The tax identification number of the beneficiary;
- The name and address of the beneficiary's payment service provider or its BIC, for payments outside the EU (European Union)/ EEA (European Economic Area); if both the name and the BIC are provided, the Bank will only use the BIC to transmit the payment to the payment service provider of the beneficiary ;
- The date of issue, that must be unique, possible and certain;
- The fees box (fill in with OUR/BEN/SHA) as mentioned above.

2. In case the Client is the beneficiary of a payment of transfer credit type, he/she is required to communicate to the payer before initiating the payment the following mandatory notes required for the proper performance of the Payment Order in question:

- The last/first name of the Account holder Client and the unique identification code, and the account number in IBAN format; mentioning the name of the Account Proxy as the payee does not represent correct identification, in which case the Bank reserves the right to refuse the payment. The Client shall alert the payer that only the Client who is the Account holder may be the payee;
- Information on the Bank unit holding the beneficiary Client account, the name of the Bank headquarters or, if applicable, the territorial unit and/or, if applicable, the BIC code (BRDEROBU).

3. The bank shall be exempted from any liability in case of non-execution, execution with delay or improper use of its obligations arising from this Contract, caused by the actions or inactions of third parties (such as correspondent banks, agents, etc.) or by any other reasons which cannot be attributed to the Bank.

4. The Bank is not responsible for any delays or damages in case of false or incomplete information provided by the Client, leading to the failure, improper or late performance of the Payment Transaction.

5. In the case mentioned in the previous paragraph, the Bank shall make all reasonable efforts to recover the funds involved in the Payment Transaction and is entitled to ask the Client for a fee for

the recovery operation, according to the Guide of Fees and commissions Individuals.

C.4 AUTHORIZING PAYMENT TRANSACTIONS OF TRANSFER CREDIT TYPE

1. Payment transactions ordered by the Client shall be authorized by the same or by the Account Proxy by expressing the consent under the Contract.

2. If the consent is expressed by the signature of the Client as the account holder and/or the Account Proxy, it must be in full accordance with the specimen signature given to the Bank.

3. The Bank shall rely on the actual, correct and original nature of signatures appearing on the instructions sent to the Bank in any way.

4. The Bank has no liability whatsoever for the consequences that may occur as a result of:

- Fraudulent or abusive use of signatures or the customized Security Features;
- Non-compliance with the methods of authorizing Payment Transactions as agreed in the Contract.

C.5 RECEIPT AND ACCEPTANCE OF PAYMENT ORDERS OF TRANSFER CREDIT TYPE

1. The Payment Order receipt is the time when the Bank receives the Order, if this is prior to the internal time limit (if any, depending on the operation) of a business day. The time limits related to the transactions with Payment Orders are presented on the intuitional website www.brd.ro and they are displayed in all BRD branches.

2. The receipt moment shall be deemed the day agreed between the Bank and the Client if the Client and the Bank agree that the performance of the Payment Order should start on a given day.

3. Payment Orders received after the time limit or on a non-business day shall be considered as received on the following business day.

4. The receipt of Payment Orders is considered performed:

- In the case of Payment Orders on paper, on the date of submission to the Bank unit mentioned on the form signed and stamped by the Bank.

- In case of Payment Orders sent by Remote Banking Services, when the Client has given the consent thereof under the Contract.

5. A Payment Order is deemed accepted by the Bank if received and acknowledged as valid.

6. A Payment Order is considered valid if:

- All the information needed to perform the Payment Order has been filled in;

- The Payment Order has been authorized under the Contract;

- In the Current Account indicated by the Client to make payments, there are the funds required for the payment and for the necessary commissions.

7. After accepting the Payment Order, the Bank debits the Current Account with the related amounts in order to perform the Payment Order, unless the Client agrees with the Bank for the performance of the order to start on a given day in which case the Account will be debited at the time of performance agreed with the Bank.

C.6 REFUSAL OF PAYMENT TRANSACTIONS OF CREDIT TRANSFER TYPE

1. The Bank may refuse to perform a Payment Transaction and take any appropriate action, including the cancellation or blocking of the Payment Instrument if the Bank considers that:

- The provisions of the Contract have not been complied with, including but not limited to ensuring the necessary amount for the Payment Transaction in the Account, filling out of Payment Orders with the elements necessary for its performance,

incomplete or unclear instructions or containing erasures, cuts, overwrites of any kind etc.;

- The Client did not submit any information/supporting documents required by the Bank;
- The ordered payment transaction may violate some legal provisions;
- The payment operation is suspected of fraudulent or potentially fraudulent activity, money laundering or terrorist financing;
- The Client refuses to provide the supporting documents specifically required by the Bank;
- The Client orders a payment to an entity subject to international sanctions.

2. A Payment Order the performance of which has been refused shall be deemed not received by the Bank.

3. The Bank shall notify the Client, in the shortest period of time possible, by one of the following ways: telephone, email, fax, SMS, by messages in MyBRD Net Internet banking service/MyBRD Mobile intuitional banking service and, if possible, the reasons for the refusal and the procedure for correcting the errors that led to the refusal, except the cases in which providing such information is contrary to the legal provisions in place.

4. If the refusal is objective, the Bank is entitled to charge a specific fee as per the Guide of fees and commissions for Individuals.

C.7 REVOCATION OF PAYMENT TRANSACTIONS OF CREDIT TRANSFER TYPE

1. The paying Client may withdraw the consent for a Payment Transaction after the Payment Order has been received and accepted by the Bank.

2. Exceptionally, the Client may cancel a Payment Transaction if the Parties have agreed that the performance of the Payment Order should start on a given day or at the end of a certain period provided the revocation is notified no later than the end of the business day preceding the agreed day for debiting (e.g. direct debit, standing orders).

3. The consent for successive Payment Transactions (e.g. direct debit, standing orders, etc.) may be withdrawn and any future Payment Transaction after withdrawing the consent shall be considered unauthorized.

4. Any withdrawal of the consent shall be made in writing (fax, email, simple letter) and, if the consent is withdrawn by another form of communication, the Client is required to submit the request in writing to the Bank by the end of the business day preceding the day agreed for debiting the Account; otherwise the Client may be liable for any damage suffered by the Bank.

5. In case the Client revokes the payment after giving the consent, the Bank will take the necessary steps for the revocation. If the payment has already been sent to the beneficiary's bank or the amount has already been credited to the beneficiary's account, the revocation shall be made only with its consent. The bank cannot be held responsible for the case when the beneficiary does not agree to return the amount received. For the operations related to the revocation of the payment subsequent to giving the consent, the Bank may apply a specific fee according to the Guide of fees and commissions for individuals.

C.8 THE PERFORMANCE OF PAYMENT ORDERS OF CREDIT TRANSFER TYPE

1. Depending on the type of Transaction ordered by the Client and the internal time limit for receipt by the Bank stipulated in the Contract, as well as of the moment of debiting the payer's account, the maximum period in which the Bank performs the Transaction is:

- Domestic payments: maximum T+1,
- Foreign payments: maximum T + 1 for payments in Euro or in another currency, when the beneficiary's payment service provider

is in the EU (European Union)/EEA (European Economic Area); maximum T + 3 for payments in any currency, when the beneficiary's payment service provider is outside the EU/EEA. In the calculation of these periods, the national non-business days or non-banking days as well as those of other States shall not be taken into account.

2. T represents the date of receipt of the Payment Order by the Bank.

3. The bank shall be exempted of any liability in case of exceeding the maximum term of performing the Payment Orders, as mentioned above, as a result of the external banking circuit, or in case of the request of information/supporting documents by the Bank or by the correspondent banks involved in their settlement and may determine potential supplementary actions, as well as in case of a time zone difference or any other reasons which cannot be attributed to the Bank.

C.9 LIABILITY

1. The Payment Order of transfer credit type is performed by the Bank with respect to the payee based on the unique identification code provided by the paying Client.

2. The Bank is not liable for the non-performance or improper performance of a Payment Transaction, as regards the payee, as a result of using an incorrect unique identification code provided by the paying Client. In this case, the Bank shall make all reasonable efforts to recover the funds involved in the Payment Transaction. If the recovery of the funds is not possible, the Paying Client may request in written to the Bank, all the information at its disposal and which are relevant to the Paying Client, in order to allow him to initiate legal action in order to recover the funds.

3. If the Client requests the recovery of funds as a result of his/her error, the Bank may apply a fee for recovery as per the Guide of fees and commissions for Individuals.

4. The Bank is liable to the Client for any loss caused, including any interest applied to the Client due to the non-performance or improper performance of a Payment Transaction, due to the exclusive fault of the Bank.

5. In case of a Payment Transaction unauthorized by the Client, and in case of a properly authorized Payment Transaction which is not performed or is performed incorrectly by the Bank, with respect to which the Client has notified the Bank, the Bank shall immediately reimburse, or in any case no later than the end of the next business day to the paying Client the amount related to the unauthorized or deficient Payment Transaction, and, if applicable, shall restore the Client Account that has been debited to the situation in which it would have been if the unauthorized or improperly performed Payment Transaction had not been carried out, regardless if the operation is initiated directly by the paying Client or through a payment services provider performing payment initiation services (PISP).

6. Exceptionally, the Bank is not liable when it can prove that the payee's payment services provider has received, within the time for completion agreed with the Client, the amount of the Payment Transaction in question.

7. In case of a non-performed Payment Transaction or of a Payment Transaction performed improperly, the Bank, at the request of the Client, shall act without delay in order to identify the Payment Transaction and shall inform the latter of the outcome, whether or not it is required to.

8. In the case of a Payment Operations initiated by the Paying Client, the Bank, as a payment service provider of the payee Client, shall be liable to him for the correct execution of the operation, unless he can prove that the payment service provider of the beneficiary has received the value of the Operation, in which case the latter becomes liable to the payee and immediately puts at the disposal of the beneficiary the value of the Payment Operations. If

the Bank is liable as a payment service provider of the Client, it will reimburse to the Client, without undue delay, the amount of the unexecuted or badly executed payment transaction and, if applicable, return the Account to the condition in which it would be found if the malfunctioning had not occurred.

9. In the case of a Payment Operations initiated by or through the Paying Client, the Bank, as payment service provider of the payee Client, shall be liable to him for the correct transmission of the payment order to the payment Service Provider of the payer. In this case, the Bank warrants that the value of the payment transaction is available to the Client immediately after the amount is credited to the Bank's account.

10. The Client undertakes to indemnify the Bank for any damages, losses or expenses incurred by it resulting from the violation of this Contract by the Client, including any damages, losses or expenses incurred by the Bank due to the financial responsibility of the Client for refusals to pay, within the limit stipulated by the legislation in force.

11. The paying Client bears, within the limit of EUR 30 or the equivalent in Lei, the losses relating to any unauthorized Payment operation resulting from the use of a Payment instrument that has been lost, stolen or used without any right, if the paying Client did not act fraudulently and did not intentionally breach its obligations regarding the issuance and use of the Payment instrument, including notification of its loss, theft or unauthorized use.

12. The paying Client bears all losses relating to any unauthorized Payment Transactions if such losses result from fraud or gross negligence or deliberate violation of his/her obligations under the law and under the Contract.

13. If it proves that the Bank is liable for the non-execution, defective or late execution of a payment transaction, the Bank is also responsible for the interest and commissions incurred as a result of the non-execution, defective execution or delay of the operation.

C.10 SECURITY TERMS AND CORRECTIVE MEASURES

1. The Client is required to keep safe all the customized Security Features of Payment Instruments through which the authorisation of Transactions is made.

2. The Bank shall ensure that the customized Security Features of Payment Instruments are not accessible to other Parties than the Client who is entitled to use the Payment Instrument.

3. The Client shall use the Payment Instruments in accordance with the law and the Contract governing their use.

4. The Client shall inform/notify the Bank without undue delay in case of loss, theft, unauthorized use of the Payment Instrument or any other unauthorized use, using the methods specific to each product in this Contract, under the agreed terms and conditions. The notification of the Bank may be made through the MyBRD Contact service, that is available to Clients 24/7 at the telephone numbers: 021 302 61 61 (regular rate number in any network) or *BANCA (*22622) (charged as a network call from any Orange, Vodafone, Telekom Mobile and RCS Digi Mobile number) or, if necessary, by other means agreed with the Bank.

5. The Bank may block the Payment Instrument due to Payment Instrument security reasons, if it is suspicion of unauthorized or fraudulent use, or there are other situations that present a certain risk that the Payer to be in incapacity to pay for the payment obligation.

6. The Bank shall inform the Client, including the reasons for blocking, if possible, before blocking or immediately thereafter, unless the action of giving such information would prejudice the justified security reasons objectively or is prohibited by other legal provisions.

7. The Bank shall unlock the Payment Instrument or replace it once the reasons for blocking it no longer exist.

C.11 REIMBURSEMENT FOR PAYMENT INITIATED BY OR THROUGH THE PAYEE

1. Within 8 weeks of the date on which the funds were debited, the paying Client may request the reimbursement by the Bank of a Payment Transaction originally authorised by or through a payee (including direct debit transactions) that has already been performed only if the following conditions are met:

- The authorization does not specify, at the time of its issue, the exact amount of the Payment Transaction of direct debit type;
- The amount of the Payment Transaction of direct debit type has exceeded the amount that could reasonably have been expected by the paying Client taking into account his/her previous spending pattern, the conditions of Contract and the relevant circumstances of the case;
- The paying Client provides at the Bank's request the specific items related to the aforementioned conditions.

2. Within 10 business days from the receipt of the reimbursement application, the Bank may repay the entire amount of the Payment Transaction of direct debit type or may justify, under the law, the refusal to repay the amount.

3. The paying Client is not entitled to any reimbursement if the same expressed the consent for the operation directly to the Bank and, where appropriate; the information on future Payment Transactions of direct debit type was provided or made available to the paying Client, in the agreed form, at least four weeks before the due date by the Bank or the payee.

D. PROOF OF TRANSACTIONS, STATEMENT OF ACCOUNT AND STATEMENT OF FEES

1. The Bank issues statements of account for transactions in the Client's Account.

2. The statement of account is a document issued by the Bank which includes the information in paragraphs 2.1 and 2.2.

2.1 If the Bank acts as the payment service provider of the paying Client, the information is:

- a. A reference enabling the paying Client to identify the Payment Transaction and, if applicable, information on the payee;
- b. The amount of the Payment Transaction in the currency in which the paying Client's Account was debited or in the currency used for the Payment Order;
- c. The price of the Transaction performed by the Client in accordance with the Guide of fees and commissions for Individuals;
- d. If applicable, the exchange rate used by the Bank in the Payment Transaction and the total amount of the Payment Transaction after that currency conversion;
- e. The date of currency of the account debiting.

2.2 If the Bank acts as a payment service provider for the beneficiary Client, the information is:

- a. A reference enabling the beneficiary Client to identify the Payment Transaction and, where appropriate, the payer and any information transferred with the Payment Transaction;
- b. The amount of the Payment Transaction in the currency in which the payment account of the beneficiary Client has been credited;
- c. The price of the Payment Transaction or the interest paid by the beneficiary Client;
- d. If applicable, the exchange rate used in the Payment Transaction by the Bank and the amount of the Payment Transaction before that currency conversion;
- e. The date of currency of the account crediting.

3. The statement of account is issued by the Bank and made available to the Client free of charge, once a month (in the case of the current/savings account), respectively once for each transaction cycle (in the case of the revolving account statement attached to

credit cards). The Bank makes available to the Client the account statement in hardcopy, in the territorial units of the Bank or, at the Client's request, addressed through the MyBRD Contact service, by e-mail to the e-mail address of the Client recorded in the Bank's records.

Through the account opening documentation/product-specific documentation, other ways of making the monthly account statement available may be agreed upon at the Client's request.

4. At the request of the Client/Account proxy and to the extent possible, the Bank may provide, for a fee, according to the Guide of fees and commissions for Individuals, information in addition to the information mentioned in paragraph 2 or in a more frequent way or by other means of communication than those mentioned in paragraph 3.

5. In addition to the monthly Account Statement, at the request of the Client/Account Proxy, the Bank may issue, within 72 hours of the request, account statements or lists of transactions for the days when transactions were ordered, for a fee, according to the Guide of fees and commissions for Individuals in force at the time of the request. These statements are made available to the Client/Account Proxy at the Bank unit where the same has opened the Account.

6. If the Client finds that his/her Account has registered an unauthorized Payment Transaction or a Payment Transaction performed incorrectly, which generates complaints, he/she is entitled to report the aforementioned errors as soon as possible without undue delay (max. 2 months from the date of debiting of the Account as stated in the account statement). Subsequent complaints may only be considered by the Bank in case of delays in justified cases, but no later than 13 months from the date of debiting of the account as stated in the account statement.

7. The Client may file the aforementioned complaints, in writing, at any unit of the Bank.

8. If the Client wishes to change his/her option of account statement, he/she will express his/her consent by filling in the Application for Statements of Account or by calling MyBRD Contact.

9. The Bank shall provide the Client, at least annually and free of charge, with a statement of all fees ("Statement of fees") incurred during a period of 12 consecutive months, on paper, at the Bank's counters.

In case of services related to a payment account, the Bank shall provide, within the same document, where applicable, the overdraft interest rate applied to the payment account and the total amount of interest charged relating to the overdraft during the relevant period, as well as the credit interest rate applied to the payment account and the total amount of interest earned during the previous 12 months period.

E. CLOSING OF ACCOUNTS

1. The Client may request for the Account closure, by an application signed and submitted to the Bank.

2. The Account shall only be closed after the payment by the Client of all the amounts owed to the Bank (the closing shall be performed if the account has no active products attached to it).

3. If there is a debit card attached to the Current Account or in the case of the Credit Card, the closing of the Account at the Client's request will be performed within 30 calendar days from the waiving / blocking all cards attached.

4. Client may require closing the account on which the garnishment was created by complying with the respect of the conditions for closing the account, the Bank being obliged to refund the Client only of the exempt amounts from the garnishment under the law.

Client may request closing the account if on the account has been ordered the measure of unavailability according to the law, with the following exceptions: where on the account / the monies in the account have been instituted protective measures by the bodies of criminal prosecution or the competent criminal courts, closing the account can be done only after the Bank receives the written consent issued by those authorities, at the request of the Client.

5. Before closing the Account, the Client is required to regularise the status of the products and services attached to that Account.

6. If the Client has opted for the changing/switching of the accounts service and requires within the Authorization form, the closing of the payment account opened with the Bank, it will close the account with the following exceptions:

a) The Client has outstanding obligations in relation to that payment account;

b) The payment account has attached other services/products contracted by the Client, such as active loan products (overdrafts, loans, etc.) or other active products and services attached to that current account (cards, deposits, remote banking services, etc.).

c) The account is denied or unavailable, in accordance with the legal provisions, for the Client's fulfilment of obligations assumed by the Bank or towards third parties.

The Bank shall proceed with closing the current account only if provisions a) – c) of article 6 above mentioned are not applicable and if the bellow conditions are simultaneously met:

6.1. The Client has handed over all BRD instruments/devices through which the Account is accessed.

6.2. The conditions for closing the account/related products and services provided for in the contract between the Client and the Bank are met.

7. With the closing of the current account, all contracts related to the provision of payment services attached to it shall also cease, including direct debit, standing order and payment orders issued with future payment dates.

8. If the Bank learns of the death of the Client, by the presentation by any person concerned of his/her Death Certificate, the Bank has the right to block the Account until the conditions mentioned below are met. As an exception to the rule of informing the Bank by the submission by any person concerned of the Client's Death Certificate, the Bank reserves the right to block the Account even if the Client's death is made known through any other means (e.g. mass media), but this is not an obligation for the Bank.

9. In case of the Client's death, the amounts in the Account or deposit shall be released only to persons designated in this regard by the Certificate of Succession and only within the limits set out in it (these people shall also submit the identity documents and the Client's Death Certificate).

10. If there are several heirs with a Certificate of Succession appointed in it as beneficiaries of the amounts available in the Account and/or the deposit, the Bank will not release the amounts in the Account or terminate the deposit unless with the agreement of all the heirs.

11. The Bank reserves the right to close any of the Client's Current Accounts with exception of the Current account with basic payment services, without prior notice in any of the following cases:

a. The following three conditions are met cumulatively: 1. the Account balance is lower than or equal to 250 EUR (or the equivalent in the Account currency); 2. the absence of any Account transactions for a period of at least 6 consecutive months; 3. the lack of products attached to that Account;

b. Delays or refusals of submission of the documents or their modifications as requested by the Bank;

c. The occurrence of two payment incidents ;

- d. The failure to submit supporting documents related to the ordered Payment Transactions or presenting documents considered unsuitable for the Bank;
 - e. The violation of the Contract (see paragraph III B art. 1-15) and/or of the legal provisions.
 - f. if the business relationship/Client presents risks deemed by the Bank to be unacceptable for BRD or for the BRD Group or the Société Générale Group.
 - g. The Client displays an improper/violent behaviour towards the Bank's employees, fails to comply with the rules of civilised conduct and under such circumstances, continuing the business relation with the client may harm the image of the Bank and/or the physical or mental integrity of its employees.
12. Until the actual closing of the Account, the Client shall regularise the status of the amounts in that Account, i.e. either transfer the amounts to another Account or withdraw them in cash. If the Client does not opt for one of these two options until the actual closing of the Account, the Client declares that he/she is aware and agrees that the Bank should close the Account and the amounts in the account on the closing date shall be kept available to the Client in a Bank account, the cash withdrawal operation being charged according to Guide of fees and commissions for individuals. No amounts resulting from the Client account closing, as specified before, shall be paid any interest from the time of the account closing.
13. The Client's right (including when this right is exercised by the heirs appointed in the Certificate of Succession) to ask the Bank to return the amounts found in the accounts at the time of their closing following the Bank's initiative subject to the conditions referred to in sub-sections 8 and 9 of this section, shall be subject to a time-limit as provided for by the Civil Code, of 5 years from the time when the Client is notified to that effect by the Bank via a registered letter with acknowledgment of receipt.
14. If the Client has previously had accounts closed for which measures of enforcement by attachment had been established, the Bank reserves the right not to open new accounts for a period shorter than three months from the closing of the accounts affected by the attachment.
15. If after the full payment of the loan/deposit liquidation the Client wishes to keep the related Current Account, he/she will express his/her expressly option by filling in the Bank's forms.
16. The Bank offers the Client, free of charge, a letter to show that all contractual obligations of the latter to the Bank have been settled.

III. RIGHTS AND OBLIGATIONS OF THE PARTIES

A. RIGHTS OF THE CLIENT

1. To receive the interest established under the regulations of the Bank for the cash available in the Account.
2. To replenish the Account by cash deposits at the Bank units or by credit transfers from other accounts opened with the Bank or other Banks. Replenishing payments in foreign currency shall be made subject to the provisions of the Foreign Exchange Regulation of the National Bank of Romania and the regulations on foreign exchange transactions in force at the time they are made.
3. To order transactions with the amounts in the Account in compliance with the Contract and the laws in force.
4. To require the closing of the Account only after the payment to the Bank of all the amounts owed to it.
5. To be provided with the statement of account evidencing the Transactions performed by the Bank.
6. To request products and/or services to be attached to the Account subject to the conditions set by the Bank.

7. To benefit from preferential conditions for a defined period of time as a result of a promotion or the entry into an agreement for the payment of salaries or other monetary rights. At the end of the promotional period/validity of the agreement or on the termination of the agreement by the Client, the standard pricing conditions in force at that time or the terms of the agreement or the documents related to the promotion shall apply.
8. To receive, upon request, during the Contract, the General Banking Terms and the Guide of Fees and Commissions.
9. To request, in any moment, on paper or another durable medium, the Fee information document and the Glossary containing the most representative services related to a payment account and their definitions.
10. To receive the Statement of fees incurred during the previous 12 months period.
11. To receive electronic messages from the Bank informing him/her on the exchange fees, if case, and the exchange rate applicable to operations performed in an EU currency other than the one of the Account attached to the card, via any of the communication channels set out according to the Contract as well as to waive the receipt of such electronic messages.

B. OBLIGATIONS OF THE CLIENT

1. To know and comply with these conditions of performance of transactions in the Account and the provisions of the other agreements concluded with the Bank.
 2. To use the Account opened with the Bank to perform Transactions using only the standard forms of the Bank. They shall be properly filled in and shall reflect real transactions, and the Client shall be responsible for this as well as for the legality/legitimacy of the operations carried out through the Account.
 3. The Client/Proxy shall provide the Bank in due time with accurate data, information and documents which the latter requests whenever deemed necessary in order to open each Account, product or service provided and to verify the legality of the transactions made through Accounts (debit and credit) and of the beneficial owner. If the Proxies submit to the Bank a special power of attorney, a power of attorney, etc. (documents provided for by the law in force) to open Accounts/ update data in the name of the holder Client, they have to submit to the Bank the required documents and information both for themselves and for the Client who is the Account holder.
- Non-resident Clients shall also provide the original certificate of tax residence issued by the tax authority from the country of residence by the first interest payable and every year after that by the 10th of February to enjoy the income tax decrease. Likewise, non-resident Clients shall notify the Bank of any change of the tax residence and tax identification number (TIN) assigned to it or functional equivalent if there is no tax identification number available (or, if applicable, why it may not be supplied), and any change in tax residence.
4. To notify the Bank of any changes to the information provided to the Bank (e.g. identification data of the Client and/or Account Proxy, the revocation of the power of attorney, etc.) and to properly replace the documents originally submitted within five business days from the date of that change. Until the receipt by the Bank of such changes from the Client, the Bank is entitled to consider the information and identification data in its possession as valid. The Bank may not be held liable for any damage caused as a result of the failure to notify in a timely and safely the changes/additions or if they have been communicated to the Bank by the Client without being accompanied by supporting evidence.
 5. To comply with the public opening hours of the Bank, as shown in its units.

6. To timely pay the bank fees, charges and interests relating to the transactions performed and products held under the Guide of fees and commissions for Individuals and the List of interests in force at the time of payment, existing at the Bank offices, on the Bank institutional website or on the Remote Banking Services website. The Client Account Holder understands that he/she is the main responsible for paying the fees and commissions owed to the Bank under the Contract. In the alternative and only if he/she fails to comply with the obligation to pay such amounts, he/she irrevocably and unconditionally authorizes the deposit in his/her account of the amounts required for paying the fees/commissions by any of the Proxies appointed for that account. In this respect, he/she agrees that the Bank, upon the request of any Proxy, can offer the latter details on the amount and type of commissions.

7. To be regularly informed about the changes in the fees, charges and interests from the postings at the Bank units, on the Bank institutional website or via the Remote Banking Services.

8. To perform operations in the Current Account or the Revolving Account.

9. To perform operations only within the limits of the available funds in the Account, including the amount of the fees and charges relating to the management of the Accounts and Transactions.

10. To perform replenishing payments at least at the level of the unauthorized overdraft (if applicable) and of the fees and related interest for the Transactions in the case of an overdraft.

11. To conduct at least one monthly replenishing payment for the Revolving Account with an attached credit card covering at least the minimum amount highlighted in each account statement, calculated by the Bank based on the credit line used (an amount including all fees, fees, charges, the insurance premium, the interest relating to the transactions and unauthorized overdraft, if applicable).

12. To be informed, at least monthly, of the Account situation, by any means made available by the Bank, including by analysing the statement of account.

13. To promptly notify the Bank of any Payment Instrument that is lost, stolen, destroyed or cancelled, so that the latter might take the necessary steps to make its further use impossible.

14. The Client irrevocably and unconditionally authorizes the Bank to recover from any Account opened with the Bank, whether current or deposit (even one which has not reached maturity), the amounts representing the payment obligations to the Bank. For the deposit accounts which have not reached maturity, the amounts remaining after the payment of the Client's obligations to the Bank shall be transferred to the Current Account via which the deposit was established and shall be subject to the interest rate applicable to the Current Account.

15. The Client understands and accepts that in case of exceptional changes in the circumstances underlying the start of the relationship with the Bank, beyond the control of the Bank, the performance of his/her obligations to the Bank shall become more onerous due to the rising costs of their performance.

16. The Client agrees to assume the risk of such circumstances occurring, and is bound to fulfil the obligations to the Bank regardless of such exceptional changes of the circumstances underlying the start of the relationship with the Bank.

17. To provide the Bank with the documents requested by it as original documents or as notarised copy or, where appropriate, in any other form required by the Bank.

18. To fill in and present the FATCA forms requested by the Bank both on starting the relationship with the Bank and on updating the data and information. The Client account holder shall complete and submit both to enter into a relationship with the Bank and to update data, CRS Information, as required by law.

19. The Client declares that (s)he has taken note of, and agrees, that the Bank may record and store audio and/or video conversations

and electronic communications between the Client/Proxy and the Bank. The Client declares that (s)he has informed, and obtained the consent of, the relevant persons (the Proxy) for the recording of the audio and/or video conversations and electronic communication messages. The Client also agrees irrevocably and unconditionally that these recordings are admissible and conclusive evidence (including in court) regarding the content of the recorded conversations/messages and may be used in any judicial, extrajudicial, administrative or arbitration proceedings. The Client has the right to refuse the recording of the conversation at the time of its initiation, in which case, the communication shall be resumed by other means of communication available to the Parties.

C. RIGHTS OF THE BANK

1. To ask the Client/Account Proxy for the documents regarding the purpose of the bank services to be carried out via the Bank.

2. To refuse to open accounts or conduct transactions ordered by Client/Account Proxy if the Bank KYC and Client acceptance policy is not observed.

3. To consider any payment made in its favour from the date of registration of the amount in the account.

4. To ask in writing for information about the Client or/and the Account Proxy in cases where there are gaps in the information held by the Bank or when the Bank considers that the information held on the aforementioned persons is not complete, accurate or is contradictory.

5. To suspend the performance of any operation in the Client's account starting from the date of the request referred to in sub-section 4 up to the receipt of all required information in terms satisfactory to the Bank. If the Client does not provide the information by the deadline specified by the Bank or the provided information is not satisfactory/ sufficient or is subsequently found not to be true, the Bank reserves the right to reconsider its relationship with the Client, including by closing his/her accounts.

6. To modify:

- The management fee for the current account attached to a loan or deposit;

- Transaction fees (related to those products/services for which the Client has the right to choose - e.g. credit transfers, payments) and to inform the Client by posting at the Bank units, on the institutional website or via the Internet banking service.

7. To retain, without this being an obligation for the Bank, from any account of the Client opened with the Bank, the owed fees, interests, penalty interests, bank charges, the equivalent value of the amounts representing unauthorized overdraft, as well as outstanding loan instalments, without any prior notice given to the Client if the account specified by Contract does not have the amounts required to cover such expenses and, where appropriate, to carry out foreign exchange transactions at its own exchange rate to buy foreign currency/RON and to replenish the Client's current account in foreign currency/RON. The Client shall not be exempted from the payment of any penalties for the amounts due or from the registration thereof with entities that collect data on Clients' creditworthiness.

8. To make payments from the Client's accounts opened with the Bank (excluding the Revolving Account), without the consent thereof, on the basis of judgments or arbitral awards, both final and enforceable, and other enforceable titles provided for by law, following a request of the entitled persons/entities.

Also, if the Client receives, in the account opened with the Bank, any pensions, disability allowances or other similar payments, allowances, incentives or other social aids, at the request of the paying institution, the Bank has the right to withhold the amounts incorrectly credited in the Client's account, including after his/her

death, without the prior consent or notification of the Client and/or of his/her heirs, and to return such amounts to the requesting paying institution. Any disagreement or dispute regarding such refund requests will be settled between the Client/his/her heirs and the paying institution, without involving the Bank.

9. To block the Client's Current Account in case of not replenishing the overdraft for three consecutive months and in case of recording an unauthorised overdraft for the current account, blocking also the card usage. The current account will be unlocked as soon as the cause that led to its blocking ceases, and the card can be used the day after the card is unlocked. Furthermore, to block the Revolving Account with an attached credit card if the Client does not replenish the mandatory minimum payment amount, within the deadline set in the contract for providing the credit card.

10. Not to use its own funds in any transactions ordered by the Client/Account Proxies and it may not be held liable for the consequences resulting from the failure to perform the transactions due to the lack of funds in the Client's account.

11. To refuse to perform any transaction in the account if it has suspicions about the Account Proxies on the nature of the transaction and also if the underlying documents present suspicious elements.

12. To transmit to the Credit Bureau, the Payment Incident Register, the Central Credit Register all risk information and the information on loan products, fraudulent activity and information about the inaccuracies from the documents/statements recorded on behalf of the Client/Account Proxies for processing and consultation whenever necessary.

13. To calculate late payment charges for the amounts owed to the Bank by the Client, all of which may exceed the amount owed by the Client. The level of those charges is different for each type of payment obligation and is posted at the Bank offices.

14. To grant the Client preferential rate conditions based on the fulfilment of eligibility conditions laid down by the Bank, which have been communicated to the Client. If the Client no longer complies with the conditions of eligibility, the Bank has the right to apply the standard rate conditions from the date when the Client no longer complies with those eligibility conditions.

15. The Bank may carry out any power of attorney, authorization, instruction such as a power of attorney given by the Client by means of the Bank's staff or a subsidiary thereof, by means of a correspondent credit institution or another credit institution.

16. Each power of attorney, authorization, statement such as a power of attorney given by the Client to the Bank is deemed irrevocable unless the Parties expressly agree in writing on the possibility of revocation.

17. The Bank may offset any outstanding obligation due by the Client to the Bank against any payment obligation of the Bank to the Client, regardless of the place of payment, the branch where the payment is made or the currency of any obligation. If the obligations are in different currencies, the Bank may convert any obligations into another currency so as to perform the offsetting using the exchange rate that the Bank uses on the offsetting date, in the normal course of its activities for similar transactions.

18. If between the Bank and the Client there are several legal relations or more accounts, the Client will not be able to perform an offsetting between asset and liability balances without the consent of the Bank. The Bank and the Client expressly agree that in the legal relations between the Bank and the Client there will be no offsets between asset and liability balances, except to the extent that the Bank gives its prior written consent on a specific offsetting operation.

19. To submit information for banking secrecy within the meaning of Emergency Ordinance no. 99/2006, by third parties (including ANAF) in the terms and conditions stipulated by the provisions of

these General Banking Conditions and/or any other legal provisions that compel the Bank to transmit such information.

20. The Bank has the right to take any action it deems appropriate to ensure, anywhere in the world, the fulfilment of obligations regarding the prevention and combating of fraud, money laundering, financing of acts of terrorism, tax evasion, as well as those regarding the provision of services. to persons who may be subject to International Sanctions. This may include, but is not limited to, investigations in order to determine whether a person is subject to International Sanctions, investigating the source of their funds/beneficiary, investigating and intercepting payments made to and from an Account belonging to the Client.

D. OBLIGATIONS OF THE BANK

1. To conduct the banking transactions in the Client's account ordered by the same or by the Account Proxy in writing or by any other means agreed between the Bank and the Client, but only subject to the funds in the Account and in compliance with its own rules and domestic and international banking rules and practices.

2. To debit the Account with the amount of the transactions performed in a currency other than that of the Account based on the exchange rate used by the Bank on the day of the transaction and notified to the Client by way of the statement of account.

3. To retain in its archives a copy of the application forms filled in by the Client on the goods and services contracted for at least 10 years from their receipt.

4. Not to send a Payment Instrument to the Client that has not been requested unless the Payment Instrument already submitted to the user thereof must be replaced.

5. To provide the Client upon the termination of the Contract, free of charge and without any request from the Client, with a document showing that all the obligations between the Parties arising from that contract have been settled.

6. To provide the Client, at least annually and free of charge, the Statement of fees incurred during the previous 12 months period.

7. To provide the Client, in due time, before concluding a payment account contract with the Bank, with the Fee information document on paper or another durable medium.

IV. KNOW YOUR CLIENT, PREVENTION OF MONEY LAUNDERING AND TERRORISM FINANCING

1. The Bank shall not open or operate anonymous accounts for which the identity of the Client who is the holder or the beneficial owner is not known and properly highlighted or accounts under fictitious names.

2. On starting a Bank-Client relation, on opening accounts or providing services and for determining the circumstances and purpose of the transactions, the Bank may ask the Client/Account Proxy whenever it deems necessary the submission of supporting/additional documents to verify their identity, to demonstrate the transaction/operation performed, identifying the source of the funds, the purpose and nature of the transactions made via the Client accounts and/or determine the beneficial owners of those transactions.

3. The Bank reserves the right to refuse transactions in/from the Client's accounts or to terminate the Client relations in the event of misrepresentation or suspicions about the truthfulness of the information declared by the Client/Account Proxy, including when they present to the Bank Payment Instruments that can be deemed as potentially fraudulent, causing payment risks, including those instruments that may affect the finality of the settlement as they are subject to sanctions provided for by the laws in force.

4. The Client is required to update his/her personal data for the entire duration of the Contract, including on his/her acquiring the capacity of U.S. resident under the FATCA reporting requirements. The Client account holder shall update data with CRS Information on the entire duration of the Contract. If the Client/ Client account holder does not comply with the obligation thereof to update the personal data, the Bank has the right not to perform the requested transactions.

Based on the information and documents submitted by the Client, provided that they meet the legal requirements, the Bank shall update the personal data thereof. The update of the data and information is a continuous process which is performed with the participation of the Bank and of the Client and the latter is required to provide the Bank with any document which may be requested.

5. In the event that a Client is represented in the relationship with the Bank by another person acting as an agent, guardian or in any other capacity, the Bank shall also obtain and verify the information and documents about the identity of the representative and, where appropriate, those relating to the nature and limits of the power of attorney. The power of attorney shall be granted either through the forms made available by the Bank or through a genuine notarized power of attorney.

The identity verification also applies for the beneficial owner and for the risk-based verification of the identity thereof.

6. In all cases in which the Client performs cash transactions with amounts of at least EUR 15,000 or the equivalent (or cumulative) during a banking day, the Client has the obligation to submit to the Bank the documents on the source of the funds and/or purpose of transaction and to fill in the statement on the identity of the beneficial owner.

7. Upon the request of the Bank, the client has the obligation to submit supporting documents for the transactions carried out through its accounts.

V. CONFIDENTIALITY

The Bank and the Client/Account Proxy undertake to comply with the confidentiality of all the facts, data, documents and information arising from the Client-Bank relationship, except as required by law or to resolve disputes related to card transactions.

VI. FINAL PROVISIONS

A. AMENDMENT OF THE CONTRACT

1. Any changes proposed by the Bank regarding the terms of the Contract shall be notified to the Client by any approved means of communication at least two months before the proposed date of application thereof.

2. The Bank shall consider that the amendments are accepted by the Client unless the Client notifies the Bank in writing before the proposed date for their entry into force of the failure to accept the changes.

3. In this situation, the Client has the right to terminate the Contract immediately and free of charge before the proposed date for the entry into force of the amendments.

B. DURATION OF THE CONTRACT

1 The Contract is concluded for an indefinite period.

2. The Contract terminates by:

a. Mutual consent;

b. Unilateral termination:

- By the Bank, subject to 2 (two) months notice;

- By the Client:

i. At any time during the Contract, with one month's notice, as well as;

ii. If the Contract is concluded online, through the Bank's institutional website, within 14 calendar days from the conclusion of the Contract, without penalties.

In this sense, the Client will present himself at any of the Bank's units and will complete a written request for denunciation. The denunciation can be made without the need to invoke any reason and provided that the amounts due to the Bank related to these services are paid in advance.

c. When expressly specified in the Contract or in the forms, specific contracts concluded between the Client and the Bank.

d. termination, if the Client has been found by the authorities to carry out illicit activities, of the nature of economic-financial crimes and corruption (tax evasion, money laundering, bribery, etc.) and the Bank has been notified accordingly by to the competent authorities.

e. The framework agreement for a basic services payment account may be denounced unilaterally by the Bank only if at least one of the following conditions is met:

(i) the Client deliberately used the basic services payments account for illicit purposes;

(ii) no transactions have been performed in the basic service account for more than 24 consecutive months;

(iii) the Client provided incorrect information to obtain the basic services payments account if the provision of the correct information would not have enabled such a right to be obtained;

(iv) Client is no longer a resident in the European Union;

(v) the Client subsequently opened a second payment account with a credit institution in Romania which allows him to use the services listed in Article 24 of Section B. Interpretation.

3. The termination has the effect of closing the account and all its attached products and services.

C. CLIENT - BANK COMMUNICATION

1. The correspondence addressed to the Bank by the Client shall be effected by registered letter with acknowledgment of receipt or by other means acceptable to the Bank (depending on how the Bank agreed in the contracts/forms related to the products/services).

2. The registered letter shall be sent by the Client to the unit where the Current Account/Revolving Account thereof is opened, as mentioned in the account opening form.

3. The Client shall always ensure that the notices thereof sent to the Bank reach the destination by the deadline set to be considered by the Bank.

4. The documents drafted in foreign languages shall be presented to the Bank together with their translation into Romanian and the notarization by a Notary of the sworn translator's signature.

5. Unless otherwise provided by specific contracts/documents concluded with the Bank and/or by mandatory legal provisions, the transmission of correspondence/notifications to the Client by the Bank will be considered performed in any of the following cases:

- The Bank has a copy of the correspondence signed by the Client;

- The respective correspondence/notification is highlighted in a shipping document signed by the courier companies or postal mandate;

- It was received by the Client on the date the Bank sent it through alternative channels (the Bank's website www.brd.ro, MyBRD Contact/phone, e-mail, fax, SMS, MyBRD Mobile mobile banking service, MyBRD Net internet banking service, YOU BRD online banking service etc.).

6. The correspondence sent to the Client by the Bank is considered properly addressed if it is sent to the last address or the last

telephone number or last email address notified to the Bank by the Client under the Contract.

7. In case the Client enters into a business relationship with the Bank online and/or the purchase of products/ services takes place in an online manner, the following are valid means of proof and may be used in any judicial, extrajudicial or administrative proceeding to prove the rights and obligations of the parties: (i) any electronic communication, sent by the Client's Bank during entering the business relationship/ contracting procedure, including by sms, e-mail, electronically displayed messages and electronic documents communicated to the Client within the dedicated internet pages of etc., (ii) any options or requests expressed by the Client and any other communications sent by him to the Bank through electronic means, in compliance with the procedure communicated by the Bank (by filling in or selecting fields in the dedicated web pages, e-mail, etc.); and (iii) any audio / video recordings made during entering the business relationship/ contracting procedure.

8. The client will be informed permanently through the specific BRD channels regarding the unavailability of a payment service and the expected term of remediation.

9. The communication between the Parties shall be in Romanian.

D. GUARANTEE OF THE FUNDS HELD

I. BANK DEPOSIT GUARANTEE FUND (FGDB)

In Romania bank's deposit are guarantee by BNR approved scheme. In compliance with art. 3, para. 1, letter h) of the Law no. 311/2015 on the Deposit Guarantee Schemes and the Bank Deposit Guarantee Fund, the deposit represents any credit balance, including the due interest, which results from funds left in an account or from temporary situations deriving from normal banking transactions and which a credit institution must repay in the legal and contractual conditions applicable, which is in none of the situations of the credit balances regulated by art. 5 of the Law no. 311/2015.

Currently, the Bank Deposit Guarantee Fund (FGDB) is the only guarantee scheme officially recognized in Romania. The guarantee of the bank deposits is regulated by the Law no. 311/2015 on the deposit guarantee schemes and the Bank Deposit Guarantee Fund.

The Bank is participating in the Deposit Guarantee Fund in the Banking System in Romania as governed by Title II of the Law 311/2015.

Depositor's debts toward BRD - Groupe Société Générale SA are taken into account when calculating the compensation payable under the terms of Title I - Deposit Guarantee Schemes of Law no. 311/2015 on the deposit guarantee schemes and Bank Deposit Guarantee Fund.

Excepted from compensation payments are the deposits included in unsecured categories as presented in the list of unsecured deposits, according with the Law 311/2015 on the deposit guarantee schemes and Bank Deposit Guarantee Fund.

Additional information is available at: <http://www.fgdb.ro/>

II. LIST OF UNSECURED DEPOSITS – ANNEX 1 LAW 311/2015

1. Deposits of a credit institution settled on its own behalf, according to the provisions of art.64 paragraph (2).

2. Instruments defined as owned funds, as these are defined at art.4, paragraph (1) point 118 from the (EU) Regulation no. 575/2013

3. Deposits resulting from transactions in relation to which final court decisions have been ruled for conviction for money laundering offences, according to the legislation in the anti-money laundering area. The classification of the deposits in this category is done by the deposits guarantee scheme, based on the information received from the competent authorities, from the credit institution whose deposits

became unavailable or from the liquidator appointed by the Court, if the case.

4. Deposits of the financial institutions, as these are defined at art.4, paragraph (1) point 26 from the (EU) Regulation no. 575/2013.

5. Deposits of the investment companies, as these are defined at art.4, paragraph (1) point 26 from the (EU) Regulation no. 575/2013.

6. Deposits for which the identity of the holder was not verified until the moment they become unavailable, according to the legislation in the anti-money laundering area.

7. Deposits of the insurers and reinsurers, as these were defined at art.2, letter A, pt.5 and 39 from the Law 32/2000 on the insurance activity and insurance surveillance with the subsequent amendments and completions.

8. Deposits of the collective investments entities as these were defined by the capital market legislation.

9. Deposits of the pensions funds.

10. Deposits of the central, local and regional authorities.

11. Transferable securities such as debt issued by the credit institution, as well as obligations derived from own acceptances and promissory notes.

E. FORCE MAJEURE

1. The Bank and the Client shall not be liable for any loss due to the disruption of the transactions in question caused by the Force Majeure.

2. The Force Majeure event is any unforeseeable, unavoidable event beyond the control of either Party, which absolutely prevents it from wholly or partially meeting its contractual obligations (e.g. natural disasters, strikes, war).

3. In case of Force Majeure, the affected Party shall communicate the occurrence of the Force Majeure event by telephone or fax, within a maximum of five calendar days, and in the next 15 calendar days it shall submit the certificate issued by the competent authorities on the Force Majeure event by registered letter or by submission to the Bank.

F. APPLICABLE LAW. DISPUTES

1. The relations between the Bank and the Client are governed by the Romanian law. Also, being part of the Société Générale Group, the Bank has the obligation to apply in relation to the Client specific regulations of the Group, including in the field of know your client, anti-money laundering and combating terrorism or enforcement of embargoes and international sanctions.

2. This Contract is written in Romanian.

3. Any dispute shall be resolved amicably by the Parties hereto. Otherwise, it shall be settled by the competent court in the territorial jurisdiction of which the Bank unit where the Client has opened the account is located.

4. If the Client considers the same injured in his/her rights, he/she may resort to extrajudicial dispute solving procedures in the following ways:

a) To notify the National Consumer Protection Authority. At the time of the conclusion of this Agreement, the address of the National Consumer Protection Authority is: Bucharest, Bd. Aviatorilor no. 72, 1st District, phone 0372131951, e-mail: office@anpc.ro, website www.anpc.ro. Additional information is available on the www.anpc.ro website, where the Client can fill-in an online referral form. The Bank cannot be held responsible for the changes in ANPC contact details. These contact details are those valid at the time of signing the Agreement.

b) To refer to the Alternative Dispute Resolution Center in the Banking Area ("C.S.A.L.B."), established by Government Ordinance no. 38/2015 on the alternative dispute resolution

between consumers and traders is an autonomous, non-governmental, apolitical, non-profit, of public interest, with legal personality, in order to ensure the access of the consumers in the banking field to the settlement, by alternative procedures of dispute resolution, of the disputes between them and credit institutions. At the time of the conclusion of this Agreement, the C.S.A.L.B. (Center) is based in Bucharest, Sevastopol no. 24, 1st District, and more information about the procedures administered by it is available at short number (021) 9414 and at the website: www.csalb.ro.

c) To seek mediation procedure under Law no. 192/2006.

d) To address the National Bank of Romania, with head office in Str. Lipscani no. 25, sector 3 Bucharest, 030031, additional information being available on the website www.brd.ro;

e) in case of differences related to the products and services of the Bank, purchased online, to use the European platform for the online dispute resolution (ODR) provided by the European Commission, by accessing the link: <https://webgate.ec.europa.eu/odr>, "Romanian" section.

5. In the event the Client submits a complaint relating to payment services, the Bank shall respond in writing within 15 business days of receiving the complaint. In exceptional situations where the response cannot be given within 15 business days for reasons beyond the Bank's will, it will provide a provisional response indicating the maximum deadline for the Bank to submit the final response. However, the deadline for receiving the final answer does not exceed 35 working days.

G. OTHER PROVISIONS

1. The Client/Account Proxy declares that the information contained in all the documents provided to the Bank is true given that false statements are punishable under the Criminal Code.

2. The Client/Account Proxy confirms that he/she has received a copy of the General Banking Terms for Individuals, the Guide of fees and commissions for Individuals and the List of Interests, and that he/she is aware of, and agrees with, the content of each clause thereof.

3. The Client/Account Proxy freely expresses his/her consent to contract, with the intent to be required under the provisions of these General Banking Terms for Individuals in their entirety and to sign these General Banking Terms for Individuals with the intent to freely obtain all the rights and obligations under these General Banking Terms for Individuals, which he/she considers to be fair. The Client declares that the Bank has made available all the documents necessary for the correct understanding by the Client of these General Banking Terms for Individuals and all aspects related thereto.

4. All the persons who are Parties of various contracts entered into with the Bank as: **legal representatives** (in the case of contracts entered into with minors), **users** (in the case of card contracts), **co-borrower or guarantor** (in the case of loan contracts) etc. state that they have received a copy of these General Banking Terms for Individuals, that they are aware of, and agree with, their content, and are subject to the applicable provisions hereof.

BANKING PRODUCTS AND SERVICES

I. NOMINAL CURRENT ACCOUNT

1. The nominal account is a Current Account or a Payment Account, inclusively a Current Account with basic payment services, opened for an indefinite period, on behalf of a single Client, with the minimum age of 18 (excluding the support current account of the package dedicated to minors aged between 14-18 years old).

2. The Client has the right to appoint Account Proxies (two persons as the standard) that may perform transactions in that account within the limits set by the empowerment.

3. This type of account is also intended for the registration of card transactions carried out under this Contract.

4. The Client is required to keep the nominative Current Account throughout the existence of the products attached to it (term deposits, loans, cards, etc.).

II. REVOLVING ACCOUNT

1. The Revolving Account (an account with an attached credit card) is the account opened automatically by the Bank on behalf of a single Client as a result of the request by the latter for the issue of a credit card.

2. The Revolving Account reflects only transactions made through the Credit Card and the fees, interests, insurance premium related thereto.

3. The Client may request up to 4 additional credit cards. The users of the additional credit cards will also act as Proxies of the Revolving Account.

III. TERM DEPOSITS

A. NOTION

The deposit account is an account opened for a defined period on behalf of a Client, with a saving function.

B. TYPES OF DEPOSIT ACCOUNTS

The Bank has in its current offer the following types of deposit accounts:

1. Term deposits with fixed interest

1.1. The interest, if the case, may be paid through one of the following methods of payment of the interest (according to the lists of interest displayed in the agencies):

- a) Every month;
- b) On maturity, with or without capitalisation;
- c) Progressively for 6 anniversary half-year periods from the date of establishment.

1.2. As preferred by the Client, term deposits may be established with two options:

- a) With an automatic renewal on maturity (except the deposit with progressive interest);
- b) Without automatic renewal on maturity.

2. Term deposits with a negotiated interest, with the interest payment on maturity (when the deposit term expires) and without an automatic renewal on maturity.

C. FEATURES

- A deposit is established/ liquidated by debiting/crediting the Current Account.

- The amounts from interest related to the Client deposits (except those for capitalisation deposits) are collected in the Current Account.

- Earnings from interest on term deposits are taxed according to the tax provisions in force.

- No partial payments and cash withdrawals are allowed from the deposit account; neither are intra and inter-bank receipts or subsequent deposits of cash into the deposit account.

- For term deposits with fixed, variable or progressive interest, the interest is calculated for a calendar year of 365 days;

- For fixed interest deposits, the interest from the time of establishment stays the same until maturity and for variable

interest deposits, the interest may vary for the duration of the deposit according to the financial and banking market.

- For term deposits with a negotiated interest, the interest is calculated for a calendar year of 360 days, except term deposits in GBP currency, for which the basis for the calculation shall be 365 days;

- The withdrawal of any amounts from the deposit before maturity entails its termination and the remuneration of the deposit at a rate of the deposit which is equal to the sight interest rate used by the Bank at the time of terminating the deposit. The amount of the deposit and the sight interest applied by the Bank at the time of termination of the deposit shall be transferred to the Current Account.

- For term deposits with fixed interest paid every month in the Current Account at the time of the termination, the Client expressly and irrevocably authorises the Bank to retain from the amount established in the deposit the difference between the interest paid every month in the Current Account until the termination of the deposit and the sight interest applicable to the amounts established in the deposit;

- For term deposits with progressive interest paid every half year on top of the funds in the deposit account (capitalisation) for six half-year periods from the date of establishment at the time of the termination the Bank shall pay the interest calculated for concluded anniversary half-year periods until the termination of the deposit plus the sight interest calculated pro rata for the current half-year period.

- If the deposit is established on a non-banking day/bank holiday, its establishment is considered to be performed on the next banking day.

- If the deposit expires on a non-banking day/bank holiday, its maturity shall be deemed to be the same day. For deposits with automatic renewal, a new deposit shall be automatically established with the interest rate valid at the time of the renewal and on the same terms as the original one. If the Client subsequently requests other conditions for that deposit, the renewed deposit shall be cancelled and another one shall be established subject to the specified conditions.

IV. OTHER SAVINGS AND INVESTMENT PRODUCTS

1. The Bank also offers to Clients other savings and investment products, as follows:

- a) Certificates of deposit;
- b) Collateral deposit accounts (deposits for payment orders with maturity, administrator guarantee deposits, escrow accounts and other collateral deposits – established guarantees);
- c) Multiplan savings-credit plan. Starting with July 4th, 2022, this product will no longer be part of the Bank's current offer. Regarding the clients who have contracted/are contracting the product before the abovementioned date, the savings-credit account will be closed at the next due date after this date, and the available funds will be transferred to the current account agreed by the specific contractual documentation.

These products are regulated individually by their respective specific bank conditions available in their respective purchase forms (contracts or documentation).

V. SAVINGS ACCOUNTS

A. NOTION

1. Savings accounts are savings products established in RON, EUR* or USD* which combine the advantages of a current account with those of a term deposit.

** The savings accounts in USD have been withdrawn from the offer starting with 01.03.2021 and the savings accounts in EUR have been withdrawn from the offer on 26.04.2021. The provisions of this Contract referring to the savings accounts in EUR and USD apply in the relation with clients purchasing this product prior to the aforementioned dates.*

B. TYPES OF SAVINGS ACCOUNTS

The Bank has in its current offer the following types of savings accounts:

1. Atustart: addressed to Clients aged 0 to 18 (not turned yet).

2. Atusprint: Savings account for Bank Clients with a minimum age of 18.

The following savings accounts have been withdrawn from sale (they are no longer part of the Bank's current offer), and the provisions of this Agreement apply to Customers who have purchased products prior to their withdrawal date, as specified below:

1. Atustart, intended for Clients aged between 0 and 14 (not turned yet). Date of withdrawal from sale: April 26th, 2021.

2. Atusprint, intended for Clients aged between 14 (turned) and 18 (not turned yet). Date of withdrawal from sale: April 26th, 2021.

3. Smart Cont:

- dedicated to Clients of at least 18 years of age, opened for an indefinite period in EUR when depositing in cash or by credit transfer for saving.

- Varying interest percentages apply depending on certain balance intervals determined by the Bank on a quarterly basis.

- Date of withdrawal from trading: September 1st, 2015.

C. FEATURES

- Savings accounts are opened for an indefinite period.

- Depending on the type, the savings accounts may have a minimum amount required for opening, in which case it will be mentioned in the specific application/documentation for opening the account. In such a case, (i) this minimum amount must be deposited in the account on the date of opening the account, otherwise the Bank reserves the right not to open the account; (ii) if, on the date of opening the savings account, the Client has outstanding payment obligations in relation to the Bank, the latter reserves the right to pay off these payment obligations first, from the amount deposited in the savings account, and to the extent that the remaining cash in the account is sufficient, the Bank shall proceed to the opening of the savings account.

- Also according to the type, the savings accounts can have a maximum ceiling for the amounts existing in the account. In the calculation of the maximum ceiling, the interests are not included.

- Minors under 14 years of age may be holders of savings accounts intended for these types of Clients (Atustart accounts) only with the consent of their Legal Representatives, but may not conduct the operations related to these accounts as these are only performed by the Legal Representatives.

- Minors aged 14 to 18 may be holders of savings accounts intended for these types of Clients and may conduct transactions in relation to these accounts with the consent of their Legal Representatives, as materialised by the signing of the specific documents.

- Savings accounts included in the current offer do not allow cards to be attached.

D. ALLOWED TRANSACTIONS

1. Deposits/withdrawals of cash in/from the savings account at the Bank units in compliance with the minimum balance in the account and/or the maximum threshold (if applicable).
2. Intra and inter-bank receipts in the savings account.
3. Payments through credit transfer from the savings account to the Current Account of the Client, opened with any Bank unit, subject to the minimum balance in the account (if applicable).

E. RIGHTS AND OBLIGATIONS OF THE CLIENT

a. Rights of the Client:

- 1 To receive, if the case, the interest determined on a quarterly basis by the Bank for the funds available in this account.
2. To designate the Account Proxy.
3. To perform, either personally or through his/her Account Proxy, the transactions referred to in art. D – “Allowed Transactions” if the empowerment does not expressly provide a limitation of the allowed transactions.
4. Transactions in the accounts whose the holders are minors shall be made in accordance with the laws in force and the guardianship court decisions.
5. The closing of the savings account is based on the written request of the Client who is the holder or of the Account Proxy.

b. Obligations of the Client:

1. To maintain (personally or through his/her legal representative in the case of Atustart, Atusprint and Atucont, if applicable), in the savings account, the minimum balance established for the currency (RON, EUR, USD), if applicable.
2. Not to exceed, personally or through his/her legal representative, the maximum threshold for the Atustart, Atusprint and Atucont accounts.
3. Not to request payments by credit transfer to other accounts than his/her Current Account.

F. RIGHTS AND OBLIGATIONS OF THE BANK

a. Rights of the Bank:

1. To determine the interest paid on the savings account, if the case, on a quarterly basis (on the 1st day of each calendar quarter). For Atustart, Atucont and Atusprint, the reference dates for the calculation of the interest are 1st and the 15th of each month and the balance to which the interest rate applies is determined by the following rules:

(a) concerning cash deposits/incomings;

(a1) cash deposits/incomings made on 1st and the 15th of each month are added to the reference balance for calculating the interest starting from those dates;

(a2) cash deposits/incomings made on any other day of the month (except the 1st and the 15th) are added to the reference balance for calculating the interest starting from the next calendar date of the 1st and the 15th;

Thus, the interest is calculated twice a month, on fixed dates: the 1st and the 15th days of the month. For the amounts deposited on any of these two dates, interest is calculated from the very moment of the deposit, and the amounts deposited or collected on any other day of the month will be taken into account for the calculation of interest starting with the next 1st or 15th day of the month.

(b) concerning cash withdrawals/credit transfer operations:

(b1) cash withdrawals/credit transfer operations made on the 1st and the 15th diminish the reference balance for calculating the interest starting from those dates;

(b2) cash withdrawals/credit transfer operations made at any other time (except the 1st and the 15th) decrease the reference balance for

interest calculation retroactive to the date of the operation, starting from the 1st or the 15th prior to that operation.

Thus, for the amounts withdrawn from the account on 1st or the 15th day of the month, the reference balance for interest calculation decreases starting from the respective dates. The amounts withdrawn on any other day of the month will be taken into account for interest calculation only until the 1st or the 15th prior to the withdrawal.

For Smart Cont, the interest is calculated on the daily balance of the account and is capitalized monthly on the 1st of each month, regardless of the date of the account opening.

2. To refuse to pay the Payment Instruments if they affect the minimum balance in the account, if applicable (except Smart Cont) or the cash deposits if they exceed the maximum threshold (in the case of Atustart, Atusprint and Atucont). If the transaction of collection in the account by credit transfer leads to exceeding the maximum permissible threshold, the Bank will inform the Client/Legal Representative within two business days. The Client/Legal Representative may collect the amount of this transaction in cash from the Bank unit where the account opening application was submitted.

3. For Atustart and Atusprint accounts, if the Client turns the maximum age allowed for that savings account, pursuant to the provisions of this Contract and without the need for further instructions from the Client, the savings account shall be closed and regarding its balance, the following can apply:

a) For products established prior to 26.04.2021:

a1) if the Client turns the maximum age allowed for the Atustart account, the Bank is authorized to open an Atusprint savings account in the same currency on behalf of the Client, under the terms of the Contract and of the costs applicable to the Atusprint account at that moment, and to transfer the entire amounts from the Atustart account in the Atusprint account.

a2) if the Client turns the maximum age allowed for the Atusprint account, the Bank is authorized to open an Atucont savings account in the same currency on behalf of the Client, under the terms of the Contract and of the costs applicable to the Atucont account at that moment, and to transfer the entire amounts from the Atusprint account in the Atucont account.

b) Starting with 26.04.2021, the savings account dedicated to underage clients (0-18 years old, not turned yet) is Atustart, the Atucont savings account is dedicated to clients of age (turned 18). If the Client turns the maximum age allowed for the Atustart account, the Bank is authorized to open an Atucont savings account in the same currency on behalf of the Client, under the terms of the Contract and of the costs applicable to the Atucont account at that moment, and to transfer the entire amounts from the Atustart account in the Atucont account.

c) Both for the products established prior to 26.04.2021 and for the products established starting with 26.04.2021, the Client understands that, in the cases considered in this article 3:

c1) If the opening of the new savings account and the transfer of the amounts existing in the closed savings account to the new account are not possible due to the failure to comply with the maximum balance specific to the new savings account:

- if at that moment, the Client holds a current account in the same currency, opened with the Bank, the amount available in the closed savings account shall be transferred in full in that current account; and

- if at that moment, the Client does not hold a current account in the same currency opened with the Bank, the amount available in the closed savings account shall be available for collection in cash by the Client in any Bank unit.

c2) The closing/opening of savings accounts and the transfer operations specified in this article 3 are free of charge and shall be

carried out on the 1st or the 15th day, immediately following the Client's anniversary;

c3) The Proxies appointed on the closed savings account shall automatically become Proxies on the newly opened savings accounts to which the transfer is being carried out.

b. Obligations of the Bank:

1. To display on a quarterly basis on the 1st of each calendar quarter, at its offices, the interest rate on the savings accounts.
2. To pay interest in the savings account of the Client (to capitalize) on a quarterly basis (on the 1st of each quarter) for Atustart, Atusprint and Atucont and every month (on the 1st of each month) for Smart Cont, respectively.
3. The gains derived from the interest on savings products are taxed according to the tax provisions in force.

VI. BANK CARD

A. GENERAL

1. The Bank offers its Clients debit cards and, where appropriate, debit cards with an Authorised Overdraft facility attached to the current accounts in Lei and / or foreign currency and credit cards. These may be used for commercial transactions, including the payment of various services and utilities and/or release of cash, both in Romania and abroad (depending on the card type).
2. The Client's request regarding the card issuance may be expressed either through the Bank's branches network or online, through MyBRD Contact service or through the institutional website www.brd.ro, by filling in the standard Bank forms. After the approval of the application by the Bank, the latter shall issue the card and the related PIN.
3. The Client Account holder is entitled to request the supply of a Card on behalf of the Account Proxy attached to the Account provided the Client Account holder is also the Holder of a Card attached to that Account. The Account Proxy may only request the same type of Card as the Client Account holder and the latter agrees that each fee associated with the Card issued in the name of the Account Proxy should be charged from the Current Account of the Client Account holder.

B. CONDITIONS FOR USE OF CARDS

1. Providing of a debit card/credit card and PIN codes

1.1. The Bank will send the Card to the Holder/User within a maximum of 90 calendar days from the date of requesting its issuance, respectively from the date of its replacement or renewal.

1.2. Depending on the option of the Holder/User, expressed at the time of requesting the Card issuance, it will be handed over to the Authorized Holder/User either (i) within the territorial unit of the Bank selected by him/her, mentioned in the card issuance documentation or (ii) by courier at the address stated for the card delivery, mentioned in the card issuance documentation, and the Client will pay the delivery fee mentioned in the Guide of fees and commissions for Individuals. The option regarding the card delivery stated by the Holder/User will also be maintained for the card renewal upon its expiry.

The holder/User may request, through the territorial units of the bank or through the MyBRD Contact Service, the change of the card delivery method. If the Holder/User requests a change of the delivery method within less than 60 calendar days before the expiration of the Card, the Bank will replace (reissue) the renewed card and will charge the card replacement fee provided in the Guide of fees and commissions for Individuals.

If the courier delivery cannot be carried out due to reasons beyond the Bank's control, the card shall be redirected to the bank unit and

the Holder/User shall be notified via SMS or by phone that he/she must take the card from the unit. The PIN will be made available by the Bank only to the Holder/User via SMS to the valid mobile number previously declared to the Bank.

In exceptional cases, the PIN will be made available by the Bank to the Holder/User in paper format, in the BRD unit where the Client has filled in the card issuing application form. The PIN related to the cards requested by the clients online, will be sent to the clients only by SMS.

1.2. To receive the PIN via SMS, the card's Holder / User will transmit after receiving the card the unique password via SMS to the phone number:

- 0371700059 (clients of the national telephone operators Orange, Vodafone and Telekom);
- 1739 (clients of the national telephone operator RCS-RDS);
- +447786201772 (clients of the international telephony operators)

The unique password is formed by the last 4 digits of the card number and the last 4 digits of the CNP (personal identification code without spaces or symbols). For non-resident clients without CNP - personal identification number, the unique password is formed by the last 4 digits of the card number and the last 4 characters of the identity document declared to BRD. In case of clients with CNP with more than 13 characters, the unique password is formed by the last 4 digits of the first 13. If the CNP contains letters, these shall be written using lower-case letters in the unique password. The SMS containing the unique password sent by the Holder/User is charged according to the standard tariff of the telephone operators.

If the mobile phone number, declared to the Bank by the card's Holder/User to receive the PIN by SMS, benefit of SMS included (for telephone operators Orange, Vodafone and Telekom), the transmission of the unique password via SMS will not involve additional costs.

The PIN via SMS must be requested via SMS with the unique password to the phone numbers mentioned above within a maximum of 90 days from the date of the card issuance. The Client will require the PIN regeneration after the expiry of this period. The PIN regeneration will be charged according to the List of fees and commissions for Individuals.

1.3 The PIN regeneration may be requested by the Card Holder/User by calling MyBRD Contact, in the Bank units or via the YOU BRD online banking service, when the latter shall have this function. Subsequent to the request, after the Holder/User is notified over the phone via message that the PIN is available, shall send an SMS to the Bank (to one of the telephone numbers mentioned above) containing the unique password (the combination of figures presented at 1.2) within 90 days from the date of the request. After the expiry of this period the Client will request another PIN regeneration. The regenerated PIN will be received by the Card Holder/User through SMS, within 24 hours from the transmission of the unique password via SMS. In order to activate the new PIN the first card transaction must be mandatorily performed by inserting the card into an ATM type terminal.

1.4 To enhance the security, the card shall be sent inactive to the Holder/User. The card shall be automatically activated upon the first transaction confirmed with the PIN code carried out in the country or abroad.

The token will be activated when the card is enrolled in a digital wallet application/service or when the card is enrolled on the websites/in the merchants' applications.

Enrolling the card in Apple Pay/Google Pay through the YOU BRD mobile banking service allows the activation of the Token even before the User/Cardholder takes possession of it.

If, prior to the reissuance (replacement)/renewal of a Card, the former Card had recurrent payments for active subscriptions or the Card has been enrolled in payment applications (e.g. PayPal, Google, AliExpress, Apple, iTunes, Uber, Wish, etc.), in order to

facilitate payments, the authorizations related to such payment types shall be automatically transferred to the new Card, without prior notification or any other formalities. The Card User/Holder must request the Card blocking and of the related Tokens if he/she no longer desires to continue those subscriptions on the new Card.

1.5 In case the Holder/User has difficulty in activating the PIN code, he/she may call the MyBRD Contact Service at any time: 021 302 61 61 (regular rate number in any network) or *BANCA (*22622) (charged as a network call from any Orange, Vodafone, Telekom Mobile and RCS Digi Mobile number).

1.6 The card may be activated at any time during its validity.

1.7 The card is the property of the Bank. The Bank may require its return or may authorize a third party to retain it on its behalf.

2. Security features. Notices for use without right or any other unauthorized use

2.1. The Holder/User shall ensure that the Card, the Security Features as well as of the devices where the digital wallet type applications/services are installed, are kept in good condition so as not to be lost, stolen, damaged or become the possession of any other person.

2.2. In case of operations performed online with the Acquirers that have implemented 3D Secure service, the Holder/User will authenticate through the mobile banking application based on biometrics or by entering the mPIN code for accessing the application. After the payment data is entered, the Holder/User will receive a notification on the smartphone in order to authenticate through the mobile banking application. The authentication for a transaction can take place for 10 minutes since the moment the transaction was initiated.

2.3. Exceptionally, for authorising the online card payments, if the Holder/User does not have a smartphone or does not have the mobile banking application, the e-commerce password shall be used. Thus, on the payment screen, the Holder/User should choose the mobile phone number (if declared several phone numbers) to receive the unique validation code for the operation. The confirmation of the operation will be done by entering the 3D Secure code in predefined field on the payment screen. If the Holder/User has not declared any phone number in the database of the Bank, or any of the numbers listed are no longer available, the transaction can not be performed. The Holder/User can transmit/communicate the Bank a new phone number to any unit of the Bank.

The Bank shall not be held responsible for unsecured online transactions for which the Acquirers choose not to request the unique code for validating the transaction or to accept payment even if the card holder/user waives it before entering the required unique validation code.

2.4. The Holder/User has the obligation to maintain and use the card safely. Thus, the Holder/User has the following obligations:

a) to take all measures for keeping the Card, customised safety features, as well as the phone/device in his/her possession and in safety conditions, if using a digital wallet type application/service where he/she has enrolled own cards, in order to protect them against loss, theft, replication, damage or use by another person. The Holder/User understands that the phone number represents both an identification key upon the registration of the user in a digital wallet type application and a secured method for the Bank to communicate with the User/Holder for sending a password via SMS, for validating the different types of operations, for example but without being limited to: enrolling Cards in payment applications (enabling the authorization of online payments, transfers, etc.), the 3D Secure code for online transactions, the Card's activation code, etc.

b) to notify the Bank immediately, without undue delay, for the loss, theft, destruction, unauthorized use of the Card/phone/device where

the payment application is installed, disclosure of the Card data/customised security features to unauthorized persons;

c) to check periodically the account situation and the transactions performed, at least once a month.

2.5. The Holder/User shall have the following obligations with respect to the use of the PIN and eCommerce password under penalty of bearing full damage:

a) Upon the receipt of the sealed envelope containing the PIN, the Holder/ User shall memorize the PIN and destroy that envelope; when the PIN was received by SMS, the PIN should be memorised and the SMS deleted;

b) if the Holder/User choose to receive the PIN on paper He/she shall immediately notify the Bank if the envelope containing the PIN has not been received sealed;

c) He/she shall not write the PIN/eCommerce password on the card or other items kept with the card;

d) He/she shall use the PIN/eCommerce password so that it should not be seen by other persons;

e) He/she shall not communicate the customised security features of the Card or the activation code received from the Bank to another person (including Bank staff, the police or other authorities), upon its verbal or written request or by accessing links received from such person via e-mail or by other means of communication;

f) If the PIN or other customized Security Feature is learned by another person, he/she shall notify/inform immediately the Bank and request the blocking of the Card and of the Tokens, if the case, and request the issue of a new card subject to the related fee. Otherwise, the Holder/User shall bear all losses in connection with any unauthorized Payment Operations, if such losses result from fraud or wilful failure or gross negligence of his obligations under these General Banking Terms.

g) He/she shall ensure the security of the work station from where the eCommerce transactions are initiated subject to the minimum conditions:

- The use of an antivirus software and an anti-spyware software with the signatures updated on a regular basis (daily) to regularly scan the computer;
- The installation and enabling of a firewall;
- The update of the system in terms of security by installing the latest updates by the manufacturer of the operating system and the latest versions of browsers (Internet Explorer/Firefox/Chrome/Safari), also updated with the latest patches.

The Bank shall never request the login or identification data of the account or the customised security features. Any such initiative shall be deemed attempted fraud and shall be reported as soon as possible to the Bank. In case of computer attacks, the Client agrees to work with the Bank for identifying the source of the attack.

2.6. The obligations regarding the keeping of the PIN/eCommerce password above also apply for the other customized Security Features.

2.7. If he/she no longer remembers the PIN, he/she must notify/announce the Bank and request the PIN regeneration (for which he/she pays a fee according to the Guide of fees and commissions for Individuals, in force at that time).

2.8. If the card/phone/device where the Mobile Banking service or the digital wallet type service/application is installed, is lost, stolen, destroyed or used without right or he/she notices an unauthorized use or disclosure of the PIN code, of the e-Commerce password or card number to other persons, the Holder/User (and the Legal Representative in case of cards issued for minors) shall notify the Bank without undue delay, in order to block the Card/Token, as follows:

a) By telephone notification of the Bank, at the MyBRD Contact Service at any time: 021 302 61 61 (regular charge number any network) or *BANCA (*22622) (charged as a network call from any Orange, Vodafone, Telekom Mobile and RCS Digi Mobile number); the MyBRD Contact service is available 24/7.

b) In case of registration of incorrect, unauthorized or fraudulent transactions, within 2 months from the date of registration of the transaction in the Account.

c) By presentation to a Bank unit for filling in the specific forms as soon as possible.

d) If the Card is lost/stolen, the User/Holder has the possibility to request the Card blocking and reissuance (replacement) also by using the YOU BRD online banking service, when this function shall be available.

e) When the Card is blocked, the User/Holder may require to keep its related Tokens in order to avoid re-enrolment in payment applications or their blocking.

f) In case of loss/theft of the device where the application in which the Card is enrolled is installed, the Holder/User must block the use of the device and to request the Bank to block the Token.

2.9. In addition to the obligations of notifying the Bank, in case of theft or loss of the Card/phone/device where the digital wallet type application is installed, as a result of which unauthorized transactions are registered, the Holder/User is required to notify the criminal investigation bodies no later than 24 hours from finding the event. If the Owner / User does not comply with the obligations expressly provided in the article, it is considered to have acted with gross negligence and shall fully bear the financial losses.

2.10. In case the Card is lost or stolen, the Holder/User may request the reissuance (replacement) of the card by telephone (the User only for own cards and the Holder for own cards and the cards of the Users via the YOU BRD mobile banking service, when this function shall be available).

2.11. The Bank shall proceed with blocking the Card of the Holder/User and of the related Tokens (upon the Client's request) immediately after being notified of the disappearance of the card/phone or device where the digital wallet type application is installed, through the aforementioned means.

2.12. The blocking of the card becomes effective after the Bank has taken adequate measures and the Holder/User who announced the case by telephone has received confirmation that the card in question has actually been blocked, as requested by the Holder/User.

2.13. The request for replacement of the lost/stolen card means that the Holder/User shall bear the related fee in accordance with the Guide of fees and commissions for Individuals, available in all Bank units and on the website of www.brd.ro.

2.14. If the Holder/User recovers the lost or stolen card after informing the Bank by telephone, the same is required to return it immediately to any unit of the Bank.

2.15. The Bank will send an SMS message to the Holder/user to confirm the atypical/suspicious transactions. If the Holder/User confirms the transaction/-s, the card can be used again, otherwise it will be blocked and another SMS message will be sent to the Holder/User for information regarding the blocking of the card, along with the instructions to follow.

If the Holder/User has not declared any telephone number to the Bank, or any of the numbers listed are no longer available, the card will be blocked from security reasons, until the transactions are confirmed by the Client.

2.16. The Bank will notify the Client by sending an SMS to the Holder/User if the card was blocked at the bank's initiative as a result of a suspicion of compromising it.

3. Using the Card

3.1. The card may be only used by the Holder/User in whose name it was issued. The card is the property of the Bank.

3.2. The Card may be used by the Holder/User starting from the receipt of the Card until the last calendar day of the month mentioned on the card.

3.3. Transactions which may be made by the Holders/Users of cards:

a) The payment for goods and/or services provided by Acquirers, which have displayed the card organization logo related to the type of card issued by the Bank (except for the Sprint card that may not be used to pay utility/service bills with vendors); For purchasing goods and services over the internet, it is recommended to trade on secured websites having the 3D Secure service implemented and displaying the logos "Verified by Visa" or "Master Card Secure code".

b) The payment to the public administration authorities who have displayed the Card acceptance logos (except for the Sprint card);

c) Obtaining cash from bank unit counters of other accepting entities upon the presentation of an identity document (if required);

d) Obtaining cash from ATMs that display the Card acceptance logos;

e) Making utility payments at the Bank ATMs;

f) Token payments: (i) contactless payments to vendors, when the card is associated to a NFC-compatible Apple/Android mobile device (smartphone, smartwatch, etc.); (ii) transactions on the Internet, on vendor websites and applications accepting card payments; (iii) cash withdrawals from terminals compatible with contactless marks.

g) Performing Quasi-Cash transactions (card transactions with a merchant in order to obtain goods that can be converted to cash convertible, such as, but without being limited to, casino chips, lottery tickets, bets, etc.);

h) Access to other optional services offered by the Bank subject to signing special requests (except the Sprint card);

i) The transfer of funds between own accounts and or third-party accounts (except the Sprint card);

j) Obtaining information on the Current or Revolving Account balance at ATMs, based on the PIN or on the answering machine line, based on MyBRD Contact Client code and password.

k) PIN change.

When performing a payment operation, the Holder/User must check the correctness of the transaction elements (amount of transaction, currency of the transaction, name of the vendor) prior to authorizing it.

3.4. For certain cards, the Bank may attach free of charge additional assistance service and insurance, which shall be made known to the Holder/User, in accordance with these General Banking Terms.

3.5. Regardless of the currency of the account to which the card is attached, it may be used both within the national and international territory:

a) Subject to the provisions of the Foreign Exchange Regulation issued by the National Bank of Romania;

b) Within the limits of the cash in the Current Account, which includes the overdrafts granted by the Bank (if any), or in the Revolving Account.

3.6. The Bank may establish usage limits for transactions made with the card that are communicated to the Holder/User in the letter accompanying the Card or in the annex to the credit card contract.

3.7. The Holder may ask the Bank to change the usage limits both for the Card issued in his/her name and for the User. This request shall be reviewed by the Bank and the decision shall be communicated to the Holder/User.

3.8. For security reasons, in order to prevent the fraudulent use of the Card, the Bank may monitor the Card transactions made by the Holder/User.

3.9. Depending on the type of Card, the Bank may require the establishment of a guarantee in the form of a sum of money frozen in the account from the collateral deposit established with BRD.

3.10. The Holder (and the Legal Representative, in case of cards issued for minors) is liable to the Bank for all payment obligations resulting from the use of the Card by any Users.

3.11. The Bank shall automatically debit the Current Account attached to the Debit Card/ the Revolving Account with an attached Credit Card with the amounts representing the value of the transactions carried out with the Card. The Client understands and accepts that, if the Card is lost, stolen or fraudulently used, this debiting shall be performed until the notification/information of the Bank by the Holder/User regarding the loss/theft/fraudulent use of the Card, except for transactions performed at terminal with offline operation, in which case the Account shall be automatically debited, as the Bank's authorization is not requested. For these transactions, if the funds available in the account do not cover the value of the transactions performed, the uncovered amount will be recorded as unauthorized overdraft.

4. Authorization and performance of Payment Transactions

4.1. A payment transaction made with the Card by the Holder/User shall be authorised by the same. A transaction is considered authorized and irrevocable by the card user by expressing consent, as follows:

- Inserting the card into a terminal that reads the chip/magnetic tape.
- By the signing the receipt and/or by entering the PIN number at Payment Terminals or by swiping the card through a POS Payment Terminal that reads the data on the chip (including in case of Offline Transactions).

- In case of transactions by means of remote communication (e.g. the Internet) through the communication of: the card number, the expiry date, CVV2/CVC2, the eCommerce password or by biometrics authentication. According to the regulations in force, depending on the risk analysis performed by the Bank, there may be cases when the strict Authentication or the eCommerce Password is not required during the payment process such as: in the case of applications/websites not using the Visa Secure and/or Mastercard Identity Check, in case of cards previously saved in the vendor's applications/websites, of recurrent payments, by Card, of subscriptions, and also depending on the payment history with that vendor or the payment amount.

- In case of contactless functionality, by holding the Card near the Terminal.

For Contactless payments that do not exceed a value set by international card organizations, it is not necessary to enter the PIN code; after every 5 consecutive contactless transactions made without entering the PIN code, the next one (the 6th transaction) shall require entering the PIN code; when the cumulative amount of consecutive contactless transactions made without entering the PIN code exceeds the value of EUR 150 (or equivalent in RON), the next transaction require entering the PIN code.

Contactless transactions made at an unassisted terminal in the European Economic Area for the purpose of paying a transport ticket or parking fee are not included in the limit of EUR 150, but without being limited to them, as well as those made at a contactless terminal outside European Economic Area.

For e-Commerce payments under EUR 30 made to a vendor within the European Economic Area, the client's consent is deemed as expressed by supplying the card data for performing the transaction. After every 5 transactions performed in this manner or if the cumulative value of the remote payment operations performed by the Client since the last application of the Client's strict

Authentication exceeds EUR 100, the Client's strict Authentication may be required.

For e-Commerce payments over EUR 30 made to a vendor within the European Economic Area, the client's consent is deemed as expressed by supplying the card data for performing the transaction. If the Client's strict Authentication is required, the Contract provisions on the strict Authentication through biometrics, mPIN or eCommerce Password shall apply.

The e-Commerce payments to a vendor within the European Economic Area may be performed without the Client's strict Authentication if the specific conditions of the European legislation in force are observed.

The Bank may not apply the strict authentication of clients in the case of a transactions carried out on the internet posing a low risk level. The risk level is determined depending on the trading profile of a Card Holder/User, which takes into account several parameters such as the amount, currency, vendor country, repeated transactions with the same vendor, to an agreed beneficiary, performance of transactions on the same device, with the same name of the card Holder/User declared, phone number, e-mail, delivery address, etc.

- In the case of Token payment transactions, the Client's consent is expressed by unlocking the mobile device by biometrics/mPIN, or, in the case of Apple Watch, by successively and quickly pressing the side button of the device twice, followed by, as the case may be: (i) for contactless payments with merchants: the proximity of the mobile device on which the Token is installed to the payment terminal of the acquirer merchant; (ii) for payments on the Internet on the websites and applications of merchants displaying the Apple Pay/Google Pay option: the agreement given on the website/in the application for completing the payment through Apple Pay/Google Pay; (iii) for cash withdrawals at terminals compatible with contactless marks, which allow the use of the Apple Pay/Google Pay: placing the mobile device on which the Token is registered near the terminal and entering the PIN code of the Card on the terminal from which the withdrawal is made.

The card Holder/User will keep the receipt or any other supporting documents in order to provide evidence in the event of discrepancies. The card holder/user is responsible for the consequences resulting from non-fulfilment of the above conditions or inadequate performance.

4.2. An incorrect entering of the PIN number, the expiry date or the CVV2/CVC2 code, three times in a row, causes Card blocking. To unlock it, the Holder/User shall contact the Bank (at any unit of the Bank, using the number written on the card or at the MyBRD Contact Bank service) or to unblock the card using the YOU BRD online banking service, when the function shall be available.

4.3. The approval of the transaction with the Cardholder determines the immediate blocking by the Bank of the related sum in order to settle it and to avoid using the same sum for other transactions. As exceptions to this, there are transactions for which the accepting entity does not require authorization from the Bank and these transactions shall be debited from the account on receiving the settlement report. The Cardholder can check the blocked amounts in the "Blocked Amounts" section through the internet banking, mobile banking service, and the ATMs of the Bank in the "Last 10 Operations List" sections. The amount blocked as a result of an operation performed with the Card will be unblocked by the Bank only with the prior confirmation of the Acquirer/its commercial bank that confirms that the transaction is not completed and will not be sent for settlement.

An amount blocked following the approval of the transaction cannot in any way be stopped from settlement because this represents the guarantee given to the acquirer bank that it will

receive its money for the amount issued by its ATM or for services provided/goods sold by the Acquirer on the date of the transaction. The initiative to settle an amount rests with the Acquirer/its commercial bank, which requests the collection of the amount by sending the transaction made through Visa/MasterCard to the issuing Bank. The transactions can also be settled by the Acquirer subsequently to the automatic unblocking of the amounts authorized from the account to which the card is attached. In these cases, the transactions shall be debited from the card account using any amounts available on the settlement date and the difference between the value of the transaction and the amounts available in the account shall be registered as unauthorised overdraft.

4.4. The date of a transaction made with the Card is the date when the transaction is registered at the Terminals. The Bank is not responsible for settling the transaction by other Merchants with an improper transaction date (other than the one at which the operation was actually performed) or with other inappropriate details of the transaction.

4.5. The debiting from the Current Account/Revolving Account attached to the Card of the amount of transactions made with the Card is made upon the receipt of the settlement report for these transactions.

4.6. In case the Holder/User is going to perform a transaction involving foreign exchange, he/she may consult/calculate the exchange rate of the date of the transaction, based on the rate displayed on the Bank website, www.brd.ro, and/or the websites of international card organizations.

4.7. The exchange rate prevailing on the transaction authorization date may differ from the exchange rate of the transaction settlement date. If, due to such exchange rate variations, the cash available in the account at the settlement date does not cover the transaction value, the uncovered amount will be recorded as unauthorized overdraft.

4.8. For international transactions (or national transactions in currency other than the account one) involving foreign exchange, the card organization performs the foreign exchange between the original transaction currency and the settlement currency, at the exchange rate determined by it at the date of transmission of the transaction for settlement. The debiting from the Current Account/Revolving Account attached to the Card of the amount of the transaction made with the card is made by foreign exchange between the transaction amount in the settlement currency and its equivalent in the Current Account currency using the exchange rate of the Bank.

4.9. The method of calculating the exchange rate for international transactions (or national transactions in currency other than the one of the account) and the exchange rate applied by the Bank for card transactions are available on www.brd.ro.

4.10. The payment obligations of the Account Holder related to card transactions made by any of the Users automatically become payment obligations in favour of the Bank and shall be reimbursed under the terms of the Contract. The Bank shall notify the Cardholder in writing on the outstanding payment obligations.

5. Chargebacks

5.1. If the Holder/User finds that his/her Account has registered an unauthorized Payment Transaction or a transaction performed incorrectly, he/she has the right to initiate the chargeback, in writing, by filling in the specific form provided by the Bank without undue delay, but not later than 13 (thirteen) months from the date of debiting the account. The Bank provides its Clients with Internet banking, Mobile banking, MyBRD SMS services, balance query services at BRD terminals (ATM/ROBO) in order to immediately identify the operations performed and to notify the Bank within the shortest time (no later than 2 months from the date the transaction was registered in the account) any unauthorised payment or

executed incorrectly. In the absence of a notification within the mentioned term it is considered that the transaction is accepted.

5.2 The Bank shall solve the Chargebacks according to the rules of card organizations and legal regulations on the use of cards.

5.3. The Bank shall notify the Holder/User of the response on his/her appeal in maximum 35 working days of receiving the written notice.

5.4. The Holder/User is required to notify the Bank of all the information and to submit all necessary documents to justify his/her chargeback, within maximum 10 calendar days from the request, otherwise, the Bank will be unable to resolve the request.

5.5. In the case of an unauthorized payment operation, the Bank shall reimburse the Client for the value of the unauthorized payment operation at the latest at the end of the next business day, after having noted or notified of the operation, unless it has reasonable grounds to suspect that a fraud exists and communicates these reasons, in written, to the Competent National Authority.

5.6. In the case of the theft/loss of the Card/phone/device where the digital wallet type application is installed, or of the fraudulent use of the customised security features as a result of which unauthorized transactions are recorded and/or in case the Bank requests the initiation of the proceedings to the police, the chargeback will be accompanied by a statement from the Holder/User regarding the actions taken by him and the proof of proceedings initiation to the Police. If the Holder/User challenges a transaction on the grounds that he/she does not recognize it/possible fraud, it is necessary to block the card in order to avoid the occurrence of other transactions of the same type. In the absence of blocking the Card, the Chargebacks initiated for the subsequent transactions will not be able to be resolved favourably. The Bank has the right to block the Card upon receipt of a notice of chargeback on the grounds of non-execution or non-approval of the transaction by the holder/user.

If the Card has been enrolled in applications (e.g. PayPal, Google, Apple, iTunes, Uber etc.) in case of any suspicion regarding the performed transactions, the User/Holder must contact the merchant directly for details regarding the respective transactions and make the proof of contacting him before initiating the Chargeback.

In case of recurrent transactions such as subscriptions, the Holder/User will ask the merchant to cancel the subscription, according to the agreed conditions. In case that, after the subscription was cancelled, the merchant continues charging, the Holder/User has the right to initiate the Chargeback accompanied by the proof of termination.

In the event of a service provider, travel agency or other provider becoming insolvent, having the legal obligation to conclude an insurance to guarantee its services, if the services paid with the Card by the Holder/User will no longer be provided, he/she will address first to the insurer mentioned in the insolvency notice for reimbursement of the amounts. If the Holder/User does not receive a response within 30 days from his/her request, he/she can initiate the Chargeback accompanied by the proof of the request sent to the insurer of the insolvent company.

The Card Holder/User is directly responsible for the transactions arising from the conclusion of a contract (by accepting the specific terms and conditions) with a merchant. The Bank cannot be held liable for direct or indirect damages suffered by the Card holder/user arising from the contract concluded with the respective merchant, which may include, but without being limited to: financial losses due to the provision of financial advisory services, losses of anticipated gains, damages to the reputation or image of the Client.

An online order for the purchase of goods/services may be cancelled only by the Holder/User initiating the order, with that vendor and in compliance with the terms and conditions agreed at the moment of the transaction. The Bank cannot interfere with this process. If the User/Holder desires to cancel an order, this step must

be initiated with the respective vendor. If the Holder/User has requested and obtained the cancellation of the order from the vendor and the amount was not reimbursed by the vendor, the Chargeback notice shall be accompanied by the proof of the vendor's confirmation of the order cancellation.

5.7. If the Chargeback is proven unjustified/ungrounded, and the value of the challenged transaction was reimbursed in the account of the Holder/User based on the chargeback initiated by him/her, the Bank will debit the account with the value of the respective payment operation and a fee will be charged for unjustified chargeback as per the guide of fees and commissions for Individuals.

6. Card blocking

6.1. The Card blocking is an operation performed by the Bank by which the use of a Card stops subject to the conditions specified below without closing the Current Account/Revolving Account of the Holder.

6.2. The Bank has the right to block the Card:

a) If transactions have not been recorded in the attached Current Account for six months, and its balance is lower than 15 EUR, the Bank will notify the Holder/User in writing at least 2 months prior to the Card blocking;

b) If the new or renewed Card is not collected within 90 calendar days from the BRD unit, without prior notice;

c) For reasons of security of Payment Instruments;

d) For reasons of suspicion of unauthorized or fraudulent use of the Card;

e) In the case of a Payment Instrument with a credit line, for a significantly increased risk that the Holder is unable to fulfil his/her payment obligation.

f) if the Bank finds repeated use of the card to perform operations that exceed the available balance of the account;

g) in case of inappropriate use of the card;

h) at the request of the competent authorities;

i) if it finds that the available balance of the account has been exceeded, the Bank being entitled also to impute penalty interest;

j) if it finds that the data provided to the Bank by the Cardholder was incorrect, incomplete or false.

k) under the conditions provided in specific contracts regarding the use of cards (for example in the case of cards enrolled in a digital wallet type application/service).

6.3. In the cases referred to in Art. 6.2, letters c), d) and e), the Bank informs the Cardholder (by any available means: telephone, fax, email, letter, etc.) in connection with its blocking and the reasons for the blocking, if possible, before the blocking and at the latest immediately after blocking the Card, unless the provision of such information compromises the objectively justified security reasons or is prohibited by other relevant legal provisions.

6.4. The Bank unlocks or replaces the Card (subject to a fee as per the Guide of fees and commissions for Individuals) with a new Card once the reasons for blocking no longer exist.

6.5. Blocking the Card of the Holder may also produce effects on the cards of the Users.

6.6. Where considered necessary, the Bank is entitled to take the following measures and shall notify the Holder/User, as soon as possible:

a) To refuse the authorization of Card transactions;

b) To cancel or block the use of the Card;

c) To replace the current Card, for security reasons;

d) To refuse providing a new Card or replace the Card without the Holder/User being relieved of any liability for transactions made with the Card by the Holders/Users.

7. Liability

7.1. In case of cards transactions, the Parties' liability operates according to the following principles:

7.1.1. The Holder/User (and the legal representative in case of cards issued for minors) is fully liable for all transactions until the notification/reporting of/to the Bank of the loss, theft or other unauthorized use of the Card and/or Security Features and shall bear any financial loss up to EUR 30 (or equivalent in RON).

7.1.2. The liability of the Holder/User is integral if it has acted negligently, in bad faith or with fraudulent intent if it has not used the card in accordance with this Contract, has not notified the Bank, without undue delay, the loss, theft, use without right or any unauthorized use of the card. The Holder/User shall not bear any loss resulting from the use of the card lost, stolen or used without right in the following situations:

- a. Loss, theft or use without right could not be detected by the Client before making the payment;
- b. The loss of the payment instrument was caused by an action or inaction of the Bank;
- c. After notifying the Bank of this event, carried out in accordance with the provisions of this Contract, unless it has acted fraudulently;
- d. The Bank did not request the strict Authentication in situations where it was required to apply this procedure.

The Holder/User has the obligation to indemnify the Bank for any debts, damages, losses or expenses if it is found that they resulted from the breach of this Contract or as a result of establishing the Holder's/User's liability for unjustifiably challenged transactions.

7.2. The Bank is not liable for any damages whatsoever that may arise from the unauthorized use of a card (lost/stolen/used without right) or if the Holder/User has acted fraudulently or failed to comply with the contractual obligations thereof on the safekeeping of the customized Security Features wilfully, culpably or with gross negligence.

7.3. The Bank may not be held liable as a result of a third party refusal to accept the payment by Card or as a result of the fact that a request for authorization of a card transaction is denied for any reason.

The Bank is not responsible for (i) the damages resulting from exceeding the available balance of the account or the limit on the use of the card, (ii) the acceptance of the card by the merchants or the refusal to accept a card, (iii) or misconduct of transactions made with the card if this delay or error is caused by third parties (for example, delayed transmission of settlement transactions).

8. Final provisions on card transactions

8.1. The Holder/User (and the Legal Representative, in case of cards issued for minors) agrees that the Bank use third-party subcontractors, processors authorized by law to act as intermediaries in relation to the Holder/User in the card payment system for the manufacturing and distribution of cards, account statements and for checking the authenticity of the card and of the Holder/User of the card.

8.2. The Contract referring to the Card is valid from the date of its conclusion and until the date of expiry of the validity of the Card held and its return to the Bank, with the possibility of automatic extension.

8.3. The Bank shall notify the Holder/User on the expiry of the validity of the Card and, if appropriate, on the automatic extension of the Contract.

8.4. On the expiry of the validity of a Card, the Contract is automatically extended, as provided for in the contract, and the Bank shall hand over to the Holder/User a new Card after verifying that the conditions set by the Bank for the Card renewal are met and if the Holder/User does not notify the Bank of the

termination of the Contract in the manner agreed under the Contract.

8.5. The Card shall not be automatically renewed if the Holder/User notifies the Bank of the Card waiver 2 months before it expires.

8.6. The termination becomes effective only after returning the Card to the Bank.

8.7. The Bank is entitled to block the balance of the Current Account (with the attached card) or the limit available in the Revolving account for a period of 30 calendar days from the date of termination of the Contract, for the purpose of settling all the transactions made prior to the termination which can be transmitted in this interval by the accepting entities. The Contract shall remain in force and shall produce effects until the settlement of all the transactions made with the Card.

8.8. The cards are automatically renewed upon the expiry of the validity only in case of a simultaneous fulfilment of the following conditions:

a) The Card is not blocked after the enforcement of the Contract provisions or as a result of the failure to comply with other contractual conditions imposed by the Bank;

b) The Current Account or the Revolving Account is not blocked due to the accounts tracking procedure;

c) The Current Account or the Revolving Account does not record unauthorized overdrafts;

d) The Holder/User meets the Bank's Credit risk criteria;

e) The Holder/User has not notified the Bank about the unilateral termination of the Contract as provided for in the Contract;

f) The existence of transactions in the last 6/12 months (depending on the Card type) on the Current Account/Revolving Account or the existence of minimum amounts available in the account, the value of the funds available being set by the Bank;

g) The Holder maintains the status of student to a university (public or private) with the following forms of education: with frequency, with reduced frequency or at distance (for BRD-ISIC cards) or of pupil/student (for Card 10);

h) The fulfilment of the age conditions imposed to the Holder (in the case of cards issued for minors and the Credit Card).

In case of withdrawal from the offer of a card, the Bank reserves the right to renew the card with another type of similar card, with the prior information of the Holder/User.

8.9. If the Bank identifies lending transactions in the Client's Account which cannot be justified by the Transactions performed by that Card, it may block these amounts over a maximum of 30 days to investigate the nature of the Transaction(s).

8.10. The termination of the Contract for the Card becomes effective only after the return of the Card by the Holder/User.

8.11. The Contract regarding the Cards is terminated as of right in case of failure on part of the Holder to collect the newly issued, rebuilt or renewed Card within the period set by the Bank.

8.12. The use of Cards for illegal purposes is prohibited, including the purchase of goods or services prohibited by law including by the applicable law in the country where the card is used.

8.13. The Contract regarding the Card is an enforceable title in accordance with the banking laws in force.

8.14 To perform IT system optimization works or for different technical reasons, the Bank may discontinue the operation of the card transaction system. In this period, the use of cards will no longer be possible at ATMs, at devices for card payments at the vendors, online payment etc. The Bank shall notify its clients of such interruptions via the website www.brd.ro.

C. SAVINGS DERIVED FROM USING CARDS AT POS

1. Notion

By way of the Savings Service related to using the card at POS (hereinafter referred to as the Service) the Client or the User of a

Debit Card attached to a Current Account may automatically transfer a sum of money from the Current Account to another Current Account – Practicont/the Savings Account for any payment made by card.

The Account in which one may save means the following products: Current Account – Practicont, Atustart, Atusprint, Atucont, Smart Cont in all currencies on offer from BRD.

2. Operating conditions of the service

2.1. In this Service, all debit cards for individuals offered by BRD are accepted.

2.2. The currency of the Current Account may be different from the currency of the Savings Account.

2.3. The Service becomes active from the date of signing the Contract/Request whereby the Client expresses his/her desire to purchase this service.

2.4. The Service changes take effect from the day following the signing of the Contract provided by the Bank for this purpose.

2.5. The closure of the Service may be done at any time by the Holder/User and shall take effect from the day following the signing of the form provided by the Bank for this purpose.

2.6. The transfers from the Current Account – Practicont/Savings Account, related to POS payments, shall be made at the end of the day.

If there are no available funds in the account, the amount determined by the Holder/User cannot be transferred in full or the Current Account – Practicont/Savings Account has been closed, the transfer cannot be performed. In the case of savings accounts for minors, on reaching the maximum threshold allowed for savings, the transfers shall no longer be performed and the clients in this situation shall be notified.

2.7. In case of lack of available funds, the Service shall NOT close, and the transfers that have not been made shall not be made retroactively.

2.8. In the case of transfers between accounts with different currencies, the exchange rate used for the transfers shall be the BRD exchange rate for account transactions (applied to payments from alternative accounts, transactions via internet and mobile banking, card payments, etc.), existing in the system at the time of the transfer and highlighted in the account statement. This exchange rate is visible on the BRD website, in the Exchange rate section, under the name of "card transactions" exchange rate.

2.9. The order of taking from the Current Account: the sums to be transferred to the Current Account – Practicont/Savings Account shall be taken last, after the loan instalments, outstanding debts, other due debts.

2.10. If the POS transaction is cancelled on the day of the payment to the trader, the transfer to the Savings Account will no longer be performed given that transfers of sums to the Savings Account are made at the end of the day.

2.11 In case of chargebacks during the coming days at traders, the amount saved may not be challenged/recovered. Thus, in the case of transactions subsequently refused by the Client/trader, only the actual value of the POS transaction shall be returned to the Current Account, but the amount of the saving shall not be affected.

3. Saving methods

This is achieved by the transfer of the amounts representing:

3.1. The rounding of the amount spent at the POS up to the first amount without decimal places, i.e. the amount paid at the POS shall be rounded off to the first whole value, and the difference between the amount paid at the POS and the whole amount shall be transferred to the Current Account – Practicont/ Savings Account.

3.2. The rounding of the amount spent at the POS to the first value which is a multiple of 10, i.e. the amount paid at the POS shall be

rounded off to the first value which is a multiple of 10, and the difference between the amount paid at the POS and a multiple of 10 shall be transferred to the Current Account – Practicont/Savings Account;

3.3. The percentage of the amount spent at the POS – the Holder/User may opt for one of the pre-set values;

3.4. A fixed sum, regardless of the amount spent at the POS – the Holder/User may opt for one of the pre-set values.

VII. INSURANCES

BRD can make available to the Client, depending on his/her option, property insurances, travel insurances, medical care insurances, etc. The specific conditions of these products are subject to specific insurance documentation. These conditions are handed to the Client at the time of contracting the product, or can be provided in writing, upon request.

VIII. GRANTING OF LOANS/ OVERDRAFTS. GUARANTEES

1. The Bank may grant short, medium and long term loans to the Client, as specified in the internal rules of the Bank.

2. Loans may be consumer and real estate/mortgage loans.

3. In this regard, the Bank opens in the name of the Client separate loan accounts for each loan category based on contracts with specific terms and conditions.

4. The granting of loans/overdrafts for the Current Account/credit line attached to the Credit Card is made based on an analysis of the creditworthiness of the Client.

5. The Client undertakes to use the Bank loans only for the purposes established by the loan agreements entered into with it.

6. The loans are guaranteed in accordance with the Bank regulations.

7. The repayment of loans is made according to the loan agreements and repayment schedules or in accordance with the specific conditions for the overdraft/credit line attached to the Credit Card.

8. For loans not repaid by the set maturities, the Bank is entitled to charge penalties to the Client and proceed with foreclosing the guarantee under the terms of the loan agreement.

9. The Bank may require the early payment of the overdraft/loan/credit line in accordance with the terms of the Contract agreed with the Client.

10. The Bank may issue guarantee letters/counter-guarantees at the Client's request, based on an analysis and in compliance with the internal regulations of the Bank.

11. In all cases described above, the Client is subject to the provisions of this Contract, supplemented by those of specific contracts.

IX. THE SAFE DEPOSIT BOX

1. Definitions and Interpretation

Safe Deposit Box – the device provided by the Bank in which the Holder safely stores property under the Agreement;

Safe Deposit Box Lease Agreement (Agreement) – these General Banking Conditions along with the Agreement – Particular Conditions and the specific forms of the Safe Deposit Box rental service;

Statement – the solemn statement issued by the Holder with respect to the property which the Holder intends to store in the Safe Deposit Box and their estimated value;

Holder – the signatory of the Agreement;

User – the person appointed by the Holder to use the Safe Deposit Box for and on behalf of the Holder under the Agreement.

2. The Bank's Obligations

2.1. To provide the Holder with the Safe Deposit Box along with two access keys, under the Agreement.

2.2. To keep the Safe Deposit Box safe, ensuring its inviolability and integrity, throughout the duration of the Agreement.

2.3. The Bank does not ensure any special storage conditions on the premises intended for keeping the Safe Deposit Boxes (e.g. temperature, humidity etc.) and shall not be liable for the degrading and/or devaluing of the items stored in the Safe Deposit Box as a result of poor storage conditions as the Holder is the only one able to assess whether the conditions offered by the Bank are suitable for the nature of the property being stored. The Bank shall also not issue any documents confirming the content of the Safe Deposit Box.

3. The Holder's Obligations

3.1. To fill out the Statement, on concluding the Agreement, and to specify the categories of property to be stored in the Safe Deposit Box, as well as the value of the property as estimated by the Holder. The Contract is concluded for a specified period of time, the minimum rental period is of 30 calendar days.

3.2. To go to the Bank to sign a new Statement depicting the new situation in case, during the rental period, the categories of property stored in the Safe Deposit Box or their values change. The Holder is the only one able to fill out/sign and amend the Statement.

3.3. To ensure that the Safe Deposit Box shall not include property that may directly and/or indirectly harm the Bank or the movement/storage/keeping of which is limited or prohibited by law (e.g. toxic, flammable, explosive or radioactive substances, drugs, perishable goods, etc.).

3.4. To inform the Bank immediately about any change in the identification data thereof or the Users' identification data and to substitute the documents originally submitted accordingly, as soon as possible after such change. Until the receipt by the Bank of such changes, the Bank is entitled to consider the information and identification data in its possession as valid. The Bank is in no way liable for any potential losses caused by the failure to notify the changes/additions in due time and safely or in the event that they have been notified to the Bank by the Client without being accompanied by the supporting documents as requested by the Bank.

4. Appointment/Revoking of Users

4.1. Appointment of Users

4.1.1. The Holder is entitled to appoint several Users for the Safe Deposit Box.

4.1.2. A User may be appointed by the Holder by coming to the Bank along with the User and signing the forms provided by the Bank.

4.1.3. In exceptional cases where the Holder cannot come to the Bank for fulfilling the formalities referred to above (e.g. being immobilised due to medical causes, out of the country etc.), the appointment of the User may be performed by filling in and signing a special authenticated Power of Attorney, which shall include at least the following elements: the User's identification data (last and first names, identity document, Personal Identification Number), the specific indication of the right to use the Safe Deposit Box, the indication of the Agreement number, the identification of the Safe Deposit Box, if the Holder has more than one, and the validity of the Power of Attorney and, where applicable, the allowed operations (e.g. opening the Safe Deposit Box only once, etc.). If the Power of Attorney does not specify the allowed operations, the User shall be deemed to have been empowered to perform all the operations allowed to Users under the Agreement.

On the first access of the Safe Deposit Box, the User shall submit to the Bank the Power of Attorney and the identity document, in original, and shall sign the forms provided by the Bank.

On the expiry of the validity, the Power of Attorney shall be considered obsolete, ceasing to have effect in relation to the Bank.

4.1.4. The User may perform only operations that cover the use of the Safe Deposit Box in accordance with the Agreement, without being entitled to conduct other operations (e.g. filling out/amending the Statement, signing Addenda to the Agreement, signing notices on the termination of the Agreement etc.), except when the User is expressly empowered to perform those operations.

4.1.5. The Holder is required to inform the Users about the formalities required for the identification by the Bank on the first use of the Safe Deposit Box, as well as the conditions of use of the Safe Deposit Box laid down in the Agreement.

4.2. Revoking of the User

4.2.1. The Holder is entitled to revoke, at any time, any of the Users appointed by the same. The revoking may be performed by going to the Bank and signing the specific User Revoking Form provided by the Bank.

If the User has been appointed under an authenticated Power of Attorney or, exceptionally, the Holder cannot go to the Bank to sign the specific forms (e.g. being immobilised due to medical causes, not being in the country), the revoking of the User shall be performed, in due legal form, by sending the revoking document to the Bank. The revoking document shall include at least the following elements: the identification of the Holder, the indication of the Agreement number, the indication of the revoked User's identification data (last and first names, Personal Identification Number), the identification of the Safe Deposit Box, if the Holder holds more than one. The submission to the Bank of the User revoking document shall be performed by the communication means approved by the Parties.

4.2.2. The revoking shall only take effect in relation to the Bank after the receipt by the Bank of the revoking document.

4.2.3. The Bank shall not be liable to the Holder for any loss suffered by the latter as a result of failing to notify the Bank in due time of the revoking of the User.

4.2.4. The Client is aware that the appointment of a new User shall not automatically entail the revoking of the previously appointed User(s). The revoking of a User may only be performed expressly in one of the ways provided for in the Agreement. The Holder is the only one responsible for ensuring, throughout the duration of the Agreement, the notification in due time of the Bank with respect to any change of the list of Users appointed in relation to the Bank.

5. The Procedure of Access of the Holder/Users to the Safe Deposit Box

5.1. The access of the Holder/Users to the Safe Deposit Box is possible during the opening hours posted at the Bank unit where the Safe Deposit Box is located.

5.2. For every use of the Safe Deposit Box, the Holder/User shall identify himself/herself with a valid original identity document, and shall sign the Safe Deposit Box Opening Register.

5.3. The Bank shall grant the Holder/User access to the Safe Deposit Box only after the fulfilment of the aforementioned conditions and the completion of the internal procedures of registration in the Bank records.

5.4. In case: (i) any dispute or conflict whatsoever arises which, according to the Bank: a) prevents the unequivocal determination of the Users or the limits or validity of their mandate, respectively, or b) otherwise prevents the normal implementation of this Agreement, or (ii) the Bank receives contradictory instructions, the Bank is entitled to suspend any operation related to the Agreement and/or take any measures which it deems necessary up to the settlement of

the dispute, as evidenced by the submission of documents that are satisfactory to the Bank.

5.5. If the Bank learns about the Holder's death, the Bank is entitled to suspend the execution of the Agreement and to block the access to the Safe Deposit Box (including Users' access). These measures may be adopted starting from the date when the Bank is informed of this or when the Bank otherwise learns of the occurrence of such an event.

5.6. Access to the Safe Deposit Box for its release shall only be granted to the Holder/User or any other person expressly empowered by the Holder to release the Safe Deposit Box, based on documents attesting such right.

Upon the Holder's death, access to the Safe Deposit Box shall only be granted to the persons designated to that effect by the Inheritance Certificate and solely subject to the limits laid down in it (these people shall also present their respective identity documents and the Holder's Death Certificate). If there are several heirs with an Inheritance Certificate who have been appointed in it as having the right to access the Safe Deposit Box, the Bank shall not allow access to the Safe Deposit Box unless with all the heirs' consent.

6. The Loss of the Keys

6.1. In case of loss/theft of one of the keys, the Holder shall notify the Bank, as a matter of emergency, as follows:

a) The Holder shall go to the Bank unit where the same has opened the Safe Deposit Box to inform the Bank and to fill out the specific forms to block access to the Safe Deposit Box;

b) After informing, according to section a), the Holder shall go to the Bank unit where the Safe Deposit Box is located, as soon as possible, for moving the property to another Safe Deposit Box (depending on the availability of the Bank). Assigning a new box involves terminating the Agreement in force and entering into a new one.

The keys to the new Safe Deposit Box shall be handed over to the Holder based on the relevant Minutes.

6.2. The Holder shall bear all the costs of replacing the locking system of the Safe Deposit Box for which the keys have been lost/stolen (including the replacement of the keys), as well as the costs of changing the Safe Deposit Box, according to the Agreement.

7. Special Cases of Safe Deposit Box Opening

7.1. The Holder understands and agrees that, in certain justified cases, the Bank is entitled to proceed with opening the Safe Deposit Box even in the absence of the Holder and/or User.

7.2. The cases which entitle the Bank to open the Safe Deposit Box, under the previous provision, are as follows:

a) In case of Force Majeure or unforeseeable circumstances;

b) Due to reasons related to the reorganisation of the Bank's premises (including the relocation of that unit) if the Holder does not go to the Bank for moving the property to the new Safe Deposit Box;

c) In the event of termination of the Agreement when the Holder does not go to the Bank for releasing the Safe Deposit Box and returning the keys;

d) In any other cases where the Bank is required to do so under the applicable law.

7.2.1. The Force Majeure Event or Unforeseeable Circumstances

In the context of this chapter, Force Majeure shall mean events and/or circumstances beyond the control of the Party invoking it, which are unforeseeable, absolutely insurmountable and unavoidable and occur after the conclusion of the Agreement and cause the Bank to proceed with opening the Safe Deposit Box, as a matter of emergency, in order to try to mitigate or prevent any

damages. This includes, without being limited to: natural disasters, fires, wars, riots, strikes etc.

Unforeseeable circumstances shall mean events which cannot be foreseen or prevented by the Bank and cause the Bank to proceed with opening the Safe Deposit Box, as a matter of emergency, in order to try to mitigate or prevent any damages. This includes, without being limited to: the certainty of the Bank that the property found in the Safe Deposit Box does not meet the criteria laid down in the Agreement (i.e. the manifestation of phenomena such as gas, smoke, odour or noise emissions, fluid leakage, heating, etc.), exceptional circumstances relating to the security of the premises where the Safe Deposit Box is located requiring the emergency relocation of the Safe Deposit Box to other premises or other cases deemed by the Bank to justify an emergency intervention).

In the event of Force Majeure or unforeseeable circumstances, the Bank shall apply the following procedure:

a) To the extent possible, the Bank shall contact the Holder of the Safe Deposit Box, as a matter of emergency, by telephone or any other means of fast communication (email, fax), informing the Holder of the situation and the fact that the Bank is going to proceed with opening the Safe Deposit Box;

b) The Bank shall immediately proceed with opening the Safe Deposit Box in the presence of the Bank representatives and a Notary Public and/or a representative of the Police/another state force agent;

c) The content of the Safe Deposit Box shall be recorded in a report signed by all the participating individuals;

d) After having opened the Safe Deposit Box, the Bank shall inform the Holder about having opened the Safe Deposit Box, the situation that has justified its emergency opening, as well as the measures taken in a notice given by courier or by post, with acknowledgment of receipt, using the contact details provided for in the Agreement.

If the Bank finds that the situation which has led to the opening of the Safe Deposit Box has been caused by a violation by the Holder/Users of the obligations thereof under the Agreement, in terms of the type of property stored in the Safe Deposit Box, the Holder shall bear all the costs and expenses related to the forced opening of the Safe Deposit Box and the removal of the property thus stored, as well as any other compensation, where applicable, under the Agreement in relation to the Holder's liability and the Bank shall deem the Agreement terminated for convenience subject to the conditions laid down in the Particular Conditions.

7.2.2. For reasons relating to the reorganisation of the Bank premises

In exceptional cases where the Bank is determined, on grounds of reorganisation, to move the Safe Deposit Box to another headquarters of the Bank or to a different safe location:

a) The Bank shall notify the Holder at least three months before the date set for the reorganisation by courier or by post, with acknowledgment of receipt, using the contact details provided for in the Agreement, specifying the day when it is going to move the Safe Deposit Box.

The Holder may opt between:

(i) Accepting to move the Safe Deposit Box to the new location of the Bank, in which case the Holder shall follow up on the Bank's request within the period specified in the notice, and shall go to the Bank to move the property to the new Safe Deposit Box and shall sign a new Agreement specifying the identification data for the new Safe Deposit Box; or

(ii) Terminating the Agreement for convenience subject to the conditions laid down in the Particular Conditions, in which case the Holder shall proceed with releasing the Safe Deposit Box by the date specified in the notice.

b) In the event that, by the date specified in the notice, the Holder does not express any option, the Bank shall move the Safe Deposit Box subject to the following conditions:

(i) After the three-month period, the Bank shall open the Safe Deposit Box in the presence of the Bank representatives and a Notary Public and, where applicable, a representative of the Police/another state force agent;

(ii) The content of the Safe Deposit Box shall be recorded in a report signed by all the participating individuals. Subsequently, the content of the Safe Deposit Box shall be sealed and stored in a different Safe Deposit Box;

(iii) The Bank shall inform the Holder about having opened the Safe Deposit Box, the procedures followed and the new location of the property found in the Safe Deposit Box by giving a notice by courier or by post, with acknowledgment of receipt, using the contact details provided for in this Agreement.

All the expenses relating to the process described above are the exclusive responsibility of the Bank.

7.2.3 In case of termination of the Agreement

On the termination of the Agreement, for whatever reason, the Holder shall return all the keys received and shall release the Safe Deposit Box within no more than three business days after the termination of the Agreement. The return of the keys and the handover of the Safe Deposit Box to the Bank shall be recorded in a report signed by the Holder/Representative of the Holder.

If the Holder does not come within the period referred to above, the Bank shall attempt to contact the Holder by telephone and/or other means of fast communication (fax, email) and shall give the Holder a notice, by courier or by post, specifying the maximum period during which the same must go to the Bank for releasing the Safe Deposit Box. Until such release, the Holder shall bear the rental fee, calculated in proportion to the number of days related to that period.

After the expiry of the period specified in the notice, the Holder expressly, irrevocably and unconditionally authorises the Bank (under article 2032 of the Civil Code) to open the Safe Deposit Box, at the Holder's expense, without the authorisation of the court (notwithstanding the provisions of article 2198 of the Civil Code), in the presence of a Notary Public and, if applicable, a representative of the Police/another state force agent. The content of the Safe Deposit Box shall be recorded in a report signed by all the participating individuals. The property shall be stored safely in a sealed bag in the Bank vault.

After having opened the Safe Deposit Box, the Bank shall inform the Holder about having opened it, as well as the measures taken in a letter sent by courier or by post, with acknowledgment of receipt, using the contact details provided for in this Agreement.

The Bank may ask the court to order measures for the conservation of the items found on opening the Safe Deposit Box and their sale to the extent necessary to cover the outstanding fees and any other amounts payable by the Holder to the Bank under the provisions of this Agreement, including the loss caused to the Bank.

In this case, the Holder shall bear all the related expenses and costs under the Agreement concerning the Holder's responsibility.

8. The Parties' Liability

8.1. The Bank's Liability

8.1.1. The Bank shall only be held liable to the extent that traces of violence on the Safe Deposit Box are found and the Holder proves the loss.

If the User finds traces of violence on the Safe Deposit Box, the User shall immediately inform the Bank representative and together they shall record the findings and the content of the Safe Deposit Box at the time in a report. The User shall expressly indicate, in a separate statement, the property claimed to have been affected (e.g. missing, destroyed etc.), and this shall be correlated with the Holder's last statement as registered with the Bank. As soon as possible, ownership documents relating to such property

and/or other types of documents as requested by the Bank shall be attached to the Statement.

8.1.2. In all cases, the Bank's liability is limited to the estimated value of the property mentioned in the last Statement recorded by the Bank. If the Holder has not mentioned the estimated value of the property kept in the Safe Deposit Box in the Statement, the total compensation which the Holder shall be entitled to claim from the Bank may not exceed the amount of the fee charged by the Bank for the last Rental Period under the Agreement – Particular Conditions.

8.1.3. The Bank shall be exempted of liability:

- (i) If the Safe Deposit Box stores property that may directly and/or indirectly harm the Bank or the movement/storage/keeping of which is limited or prohibited by law;
- (ii) If cash (regardless of the currency), except coins belonging to various numismatic collections, is deposited in the Safe Deposit Box,
- (iii) In case of any losses caused as a result of failing to notify in due time the changes in terms of the Holder's or Users' data or if they have been notified to the Bank without being accompanied by the supporting documents (when requested by the Bank);
- (iv) For any direct or indirect damages invoked by the Holder due to the exercise by the Bank of the rights laid down in this Agreement.

8.2. The Holder's Liability

8.2.1. The Holder is fully liable for all the operations undertaken by the Users and the Bank shall only be responsible for verifying the identity of these persons based on the presented identification documents.

8.2.2. The Holder shall bear all the expenses and costs related to the replacement of the Safe Deposit Box locking system and, where appropriate, the costs of removing the property stored and other compensation, if the replacement of the keys/opening of the Safe Deposit box occurs due to the Holder's fault (e.g. loss of keys, breach of the obligations in terms of the type of property stored in the Safe Deposit Box, the failure, on part of the Holder/User, to show up by the due date for opening the Safe Deposit Box etc.).

8.2.3. The amount of the costs associated with the replacement of the Safe Deposit Box locking system and the payment terms shall be provided for in the Agreement – Particular Conditions.

8.2.4. The Holder expressly, irrevocably and unconditionally authorises the Bank (under article 2032 of the Civil Code):

- (i) To debit any accounts of the Holder (current or deposit accounts, even ones which have not reached maturity, expressly waiving the benefit of the term or the interest) with any amounts representing the payment obligations of the Holder to the Bank that have become due under this Agreement;
- (ii) To make any foreign exchange transactions which it deems necessary in order to recover the outstanding payment obligations, in the currency in which they must be paid and using the exchange rate applied by the Bank on the day of the relevant foreign exchange operation, and the Bank shall be empowered to sign any necessary documents on behalf of the Holder.

X. REMOTE BANKING

A. GENERAL PRINCIPLES

The Client may subscribe to various services of the Bank and may also perform certain transactions through Remote Banking Services provided by the Bank, in compliance with the applicable law and the procedures and internal regulations of the Bank. In view of complying with the national laws in terms of money laundering, the fight against terrorism and the enforcement of international sanctions, in the case of transactions performed via the remote banking system, at the Bank's request, the Client is required to submit all the required supporting documents. The Client understands that any communication/procedure for the

performance of which unsecured remote communication techniques are used shall be performed under his/her own responsibility and the Bank does not bear any responsibility in case of possible fraud.

Minors aged between 14 and 18 years old can join one of the remote banking services only with legal representative agreement materialized by signing specific documents.

The terms and conditions specific to the YOU BRD online banking service are subject to a specific contract, remotely concluded between the Client and the Bank.

1. Interpretation of specific terms of Remote Banking Services

a. Subscriber: the Client who has joined a Remote Banking Service. The Account Proxy may join some of the services as specified by the Bank and shall be subject to all applicable provisions of this Contract, with the specified limits, in the same manner as the Client who is the Account Holder.

b. AISP: payment service provider carrying out account information services.

c. Digital fingerprint (Touch ID): used by the Subscriber to log in the application of the MyBRD Mobile banking service and the authorization of the following transactions: transfers between the accounts of which he/she is the holder, foreign exchange, transfers to predefined national beneficiaries, payments of invoices, payments by QR code, establishment and liquidation of deposits, opening of current and savings accounts.

d. Security codes: Subscriber's own confidential safety means, used for the identification and for accessing the Remote Banking Services. For each service, these codes may have different features and names (e.g. User Code, Password, Fingerprint, Bank PIN, etc.).

e. Support Account: the current account specified by the Subscriber from which the Bank draws the monthly usage fee. The types of Bank accounts that can be defined as support accounts are determined by the Bank and notified to the Subscriber at the time of joining the service.

f. Transaction functions: transactions allowed to the Subscriber via the Remote Banking Services (e.g. payments performed through credit transfer). The maximum acceptable amounts for Transaction Functions shall be notified to the Subscriber upon entering into the contract for this service.

g. PISP: payment services provider performing payment initiation services.

2. Accounts that may be subject to Remote Banking Services

a. The accounts covered by the Remote Banking Services shall:

- Be valid;
- Not be subject to bank prohibitions (the presence in the Payment Incidents Register);
- Not be subject to a court ban,
- Not be blocked.

b. The accounts used by the Subscriber to join the Remote Banking Services may be subject to the Transaction Functions if during the period of the contract:

- Their banking specificity allows it;
- The Bank has not denied the access to Internet/Mobile banking services.
- The Subscriber has not notified the suspension of the access to the Internet/Mobile banking services.

3. Rights and obligations specific to Remote Banking Service

3.1 The rights of the Bank:

a. To accept the Client's request of joining Remote Banking Services only if the conditions of joining these services notified to Subscribers are met, before concluding the specific contract.

- b To restrict the access to Internet/Mobile banking services if the accounts with which the Subscriber has joined the Remote Banking Service do not meet the conditions of art. 2.
- c. To limit and modify the value of the transactions ordered by Subscriber, per transaction and per day. The transaction values are communicated to Subscribers via the Remote Banking Service used and they can take note of that before each transaction.
- d. To fill in the list of Transactional Functions without needing to sign an addendum. If the Subscriber believes that the new Transactional Functions contradict his/her interests, the same may require the termination of the specific contract.
- e. Not to intervene in disputes arising between the Subscriber and the telephone operator/Internet provider.
- f. The Bank is exempted from liability for any direct or indirect damage suffered by the Subscriber and shall not pay any damages to the latter or any third party for the following cases:
 - The infiltration of a third party in the computer system of the telephone operator/Internet provider by using fraudulent means or any other method that might cause to them, without limitation, information damage and the destruction of databases, programmes or information disclosure. The telephone operator/Internet provider has the sole responsibility for the protection of its computer system against such infiltration and is responsible for the protection and security of its own computer system.
 - Complaints and malfunctions caused solely by the error or negligence of the telephone operator/Internet provider or subcontractors thereof.
 - The transmission of information in the network of the telephone operator/Internet provider or any incidents occurring during the transmission of information during the use of the services by the Subscriber.
 - The loss of data, distortions or delays in data transmission caused by events beyond the control of the Bank.
 - The misuse of the Bank instructions, incorrect information entered by the Subscriber when requested at the time of performing the transactions and/or malfunction of its equipment.
 - Any malfunction of the services.
 - The consequences of the remote banking service disruption if the Subscriber does not address the Bank for performing the transactions by other services provided by the Bank.

3.2. Obligations of the Bank:

- a. To apply the strict Authentication of the client when it accesses its payment account online or initiates an electronic payment operation, or undertakes any remote action that might involve a risk of fraudulent payment or other abuses.
- b. To implement the means of receipt and/or issue of computerized data.
- c. To be liable for the losses suffered by the Subscriber in the conduct of transactions after receiving the notification of the Subscriber regarding the fact that third parties know its Security Codes.
- d. To be liable for the losses suffered by the Subscriber if it has conducted transactions in breach of the order given by him/her.
- e. To provide the Subscriber with a detailed list of the transactions performed in current accounts/revolving accounts through the specific service.
- f. To take immediate measures to assess, prevent and limit the risks that may occur as a result of the fraudulent use of Security Codes if the Subscriber notifies the Bank of an event among those specified in the chapter on "Obligations of the Subscriber", letter d.
- g. To notify the Subscriber of any amendment to the Remote Banking Services Contract and of any additional data needed to use the service by publication on the institution's website or, where appropriate, through the website www.mybrdnet.ro and by displaying at the Bank.

3.3. Rights of the Subscriber:

- a. To request the list of transactions performed in current accounts/revolving accounts via the Remote Banking Service.
- b. To address the Bank for transactions via other services provided by the Bank in the event of interruption of the Remote Banking Services from any cause.
- c To change the support account.

3.4. Obligations of the Subscriber:

- a. To safely maintain and use the Security Codes and identification data as the Subscriber is solely responsible for the consequences of their disclosure to or use by third parties.
- b. Not to declare Security Codes that can be easily known by third parties.
- c. To inform the Bank as soon as possible and in any way about any disclosure/use of the Security Codes to/by unauthorized third parties. All the transactions performed by the Subscriber shall be authorized based on the Security Codes to be considered by it. Entering the Security Code belonging to the Subscriber represents the unambiguous consent by the latter to the processing of the sent transactions and their consequences may not be attributed to the Bank.
- d. To notify the Bank as soon as he/she finds one of the following:
 - The account thereof has registered transactions that have not been ordered by the Subscriber;
 - There are elements that create doubts about the possibility that others might know the Security Codes.
- e. To specify a support account from which the fees and costs relating to the transactions shall be taken.
- f. To define a new support account, in case of deletion of the support account from the list of accounts accessible via the specific Remote Banking Service. If the Subscriber does not have any account he/she might choose as support account, the Contract will be terminated without any prior notice.
- g. To regularly check the additional data needed to use the service via the institution's website, the website of www.mybrdnet.ro or by posting at the Bank offices.

4. 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.

Thus, the Bank may grant to these third parties the access to the Client's Account, accessible online, without being liable for the fulfilment of obligations of such third parties.

The Bank may refuse the PISP or AISP access to a payment account if there are objectively justified reasons and evidence related to unauthorised access of the PISP or AISP to the payment account.

In such cases, the Bank shall communicate to the Client, through the means agreed in this Contract, the refusal of access to the payment account and the reasons for such a refusal.

4.1. 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 has the obligation to communicate with the PISP in security conditions and immediately after receiving the payment order on its behalf, it shall communicate all the information required for executing the payment transaction.

The Bank shall not charge differently in relation to operations initiated as such.

4.2. 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 has the obligation to communicate with the AISP in security conditions, providing it with information on the Client's Accounts accessible online.

The Bank shall not charge the Client for this service.

5. Pricing for Remote Banking Services

a. The Bank charges a monthly fee to use the service contracted as well as the fees and costs related to the banking transactions incurred through the service. They are published in the Guide of fees and commissions for Individuals.

b. The Subscriber has the obligation to pay the fees and costs referred to in letter a in force at the time of the transactions.

c. The Subscriber shall bear the cost of telephone communication/Internet service which shall be charged to the same directly by the telephone operator/Internet provider thereof.

6. Changing the Contract on Remote Banking Services

a. The Subscriber may make additions to the list of accounts used for joining that specific Remote Banking Services (list of searchable accounts, list of payments receiving accounts).

b. The Subscriber may suppress accounts from the list of accounts used for joining the Remote Banking Services provided that at least one usable account is maintained. Excluding an account from the list of usable accounts shall not have consequences on the existence of that account.

c. The changes referred to in letter a and b can be achieved if the Subscriber comes to the Bank and fills in the specific forms and by any other means provided by the Bank and notified to the Subscriber.

7. Duration of the contract, suspension, termination

a. The Contract on Remote Banking Services is concluded for an indefinite period.

b. The Bank reserves the right to suspend the access to Transaction Functions of the Remote Banking Services in the event of failure by the Subscriber to comply with the specific nature of the accounts and if the Subscriber does not ensure the availability of an amount sufficient to cover the monthly fee for the service, if any, in the account and under the terms predetermined upon signing the contract.

c. The Bank may unilaterally terminate the Contract for Remote Banking Services with 2 months' notice sent by registered letter with acknowledgment of receipt, stating the reason for the termination.

d. The Subscriber may request the termination of the Contract at any time by coming to any of the Bank units and filling in a request for the waiver of the service or via MyBRD Contact service (for cessation of services MyBRD Net and Mobile). The Subscriber may terminate the Contract within 14 calendar days of its conclusion without paying any penalties, subject to prior payment of amounts owed to the Bank for these services.

e. The Bank shall terminate the Contract without notice, (i) in case of deletion of the Contract support account from the list of accounts accessible via the Remote Banking Services and the absence of another account that may be chosen as the support account, if applicable, (ii) in any situation imposed by legal dispositions/decisions of competent authorities.

f. The Bank reserves the right to suspend/close these services immediately in the case of occurrence of risks relating to the security of the computer system of the Bank or the failure to comply with the Contract on Remote Banking Services by the Subscriber.

g. The Subscriber may, if necessary, ask the Bank to suspend/terminate the Contract for Remote Banking Services.

8. Other provisions

a. The provisions of this Chapter X "Remote Banking Services" shall be supplemented by those of the chapter "General issues on accounts", including as regards the Account Proxies.

b. The irrefutable proof for the Bank of receipt of instructions from the Subscriber, the justification of related transactions and the levying of related charges is represented by the records of the systems used to receive instructions of the Subscriber or their reproductions on computer medium or on paper (account statements printed by the Bank). The period of storage of these instructions on the Bank servers is 10 years from the date of closure of the year in which they were prepared, as required by the law in force.

c. General, economic and financial information provided by the Remote Banking Services is informative in nature.

d. Both the content of the website www.mybrdnet.ro (information, images, etc.) and the software serving the Remote Banking Services are the exclusive property of the Bank. Outside the provisions of the Bank - Subscriber Contract on how to access and operate Remote Banking Services, any activity for operating them (such as reproduction, adaptation, representation, etc.) is not allowed without the prior consent of the Bank and shall be sanctioned according to the laws in force.

B. MyBRD Contact SERVICE

The MyBRD Contact Service is a "Remote Banking" service via the "Telephone" distribution channel and can be reached at: 021 302 61 61 (regular charge number in any network) or *BANCA (*22622) (charged as a network call from any Orange, Vodafone, Telekom Mobile and RCS Digi Mobile number).

The Bank may establish specific eligibility conditions for customers who use the MyBRD Contact Service, in accordance with the Bank's policy and regulations in force.

1. Main Functions

1.1. For Bank Clients and non-Clients:

a. The possibility of finding out commercial information about the Bank's offer of products and services;

b. Setting meetings with Client Managers from the BRD unit;

1.2. For Bank Clients:

a. the possibility of obtaining customized information on the held products;

b. debit card issuing, by filling in the application forms provided by the Bank on the institutional website and/or a application by telephone;

c. amendment of the contractual conditions for MyBRD SMS, MyBRD Contact services and for the Internet banking MyBRD Net service, respectively for the Mobile banking service MyBRD Mobile, including the list of searchable accounts and the list of accounts receiving payments;

d. assistance in joining MyBRD SMS, YOU BRD internet and mobile banking service and MyBRD Contact service;

e. termination of MyBRD Net Internet banking service, MyBRD Mobile banking service, YOU BRD internet and mobile banking service, MyBRD SMS and MyBRD Contact services, with the condition of prior payment of amounts owed to the Bank for these services;

f. resetting the PIN code for MyBRD SMS;

g. blocking the card in case of loss/theft or unblocking it;

h. revocation of Proxy Account;

i. modifying the mailing data (e-mail and correspondence address);

j. blocking/unblocking contactless functionality for cards;

k. receiving requests for card reissuance in case of loss, theft, damage, demagnetization, possibly compromised or captured card;

l. taking over chargeback requests for card transactions carried out by the Client, if he/she is unable to come to a BRD unit.

m. sending by email the current account/savings account and revolving account statements, corresponding to a maximum period of 12 months prior to the date of the request, and the Client will bear the related fee according to the Guide of fees and Commissions for Individuals;

n. the purchase of a package of current account products and services, according to the Bank's offer regarding the packages of current account products and services that can be purchased this way;

o. the completion of requests for card enrollment in Apple/Google Pay applications when Apple/Google requests additional checks in the card enrollment process;

p. Apple/Google Pay token deactivation;

r. regeneration of the PIN code related to the card, sent by text message;

s. changing the daily trading limits for cards ;

t. validation of the personal and financial information declared by the client during the video session related to the process of entering into a business relationship with the Bank in the online environment, through its institutional website;

u. changing the delivery method for reissued (replaced) or renewed cards upon expiration, in the sense of their delivery to the card delivery address indicated by the client.

v. taking over the requests for blocking/unblocking accounts in case of suspected fraud.

1.3. For customers aged 14-18, the operations that can be performed through the MyBRD Contact service are limited, so letters b), d), f), h), i), m), n), s), t), u) in item 1.2 above do not apply to these and the operation stated at letter e) of point 1.2 applies only with regard to the termination of the YOU BRD internet and mobile banking service.

1.4. For customers who use the MyBRD Contact service as account proxies and who do not have a card as an Authorized User, the operations that can be performed are limited to those provided in paragraph a) of item 1.2 above.

Also, the proxy will be able to request the blocking of the account according to letter v) of point 1.2 above, but will not be able to request its unblocking.

2. Access to personalized information on the automatic answering machine service and security conditions

2.1. Access is available to the Subscriber the next business day from the signing of the Bank's standard forms, in case of subscription in a BRD agency and at the moment of phone confirmation of the Client, in case of subscription through MyBRD Contact service. In case of closure, it takes effect the second business day from the date of request.

2.2. If the Subscriber wants to automatically obtain information about the account balance and the latest transactions registered on the current account, directly on the answering machine:

a. He/she will choose the appropriate option from the telephone keyboard, according to the answering machine instructions;

b. He/she will identify with MyBRD Contact Client Code and the confidential numeric password (entered from the telephone keyboard);

c. The answering machine will notify the Subscriber about the telephone call recording.

2.3. The Subscriber's accounts used for automatically obtaining information on the answering machine are current/savings accounts that the Subscriber has opened at the Bank as a Holder or as a Proxy. Joining the accounts held as proxy to the MyBRD Contact Service is made only with the consent of the account Holder, at the BRD unit.

2.4. By this document, the Bank and the Client expressly and unconditionally agree that recordings of telephone conversations and electronic communications (emails) carried or transmitted by the means of communication agreed with the Bank are deemed to be conducted with the Client, and the information thus transmitted will have contractual value, and any agreement transmitted by that means will constitute their valid consent to the provision of the services under the agreed conditions.

Phone conversations and electronic communication messages are admitted as evidence, represent conclusive evidence of the contents of the instructions, conversations or messages thus recorded or of the transactions thus concluded and may be used in any judicial, extrajudicial or administrative proceedings.

3. Responsibilities specific to the MyBRD Contact Service

3.1. For the Bank

a. To record the telephone conversations between the Subscriber and the Bank in order to ensure the best possible quality of the service and to track the requests/agreements/options/preferences of the Subscriber regarding a particular product or banking service and also Bank's response.

b. To keep a record of the transactions performed by the Subscriber through this service.

3.2. For the Subscriber

a. To provide the Bank with complete and accurate information necessary to perform the required operations and/or to provide personalized information.

b. In order to be identified by telephone, the Subscriber has the obligation to answer the questions of the Contact Center officer, prior to the requested operation and/or the provision of personalized information.

c. To comply with the rules of civilised conduct, including (but without being limited to) the use of proper language, non-violent during the interactions with the Bank through this service.

C. MyBRD SMS SERVICE

The MyBRD SMS Service is a "Remote Banking" service accessible via the dedicated short number **1701** via the mobile telephone and covering the accessing/receiving of information on the Bank accounts or general banking information.

1. Information that can be accessed/received via the MyBRD SMS Service:

a. Information about the Bank accounts that is different depending on the type of account:

- For current and savings accounts: the date (day, hour and minute) of balance transmission, the label and currency of the account, the balance available upon submitting the information, the approved credit limit;

- For accounts with attached credit cards: the date (day, hour and minute) of balance transmission, the label and currency of the account, the balance available upon submitting the information, the due date of the loan, the interest rate;

- For loan accounts: the date (day, hour and minute) of balance transmission, the label and currency of the account, the balance available in the account (loan balance + outstanding payments), the due date of the loan, the interest rate;

- For deposit accounts: the date (day, hour and minute) of balance transmission, the label and currency of the account, the balance available in the account, the due date of the deposit, the interest rate

b. Information about the last 5 transactions (mini-statement) of a current account, savings account or an account attached to a credit card:

- Debit transactions

- Credit transactions
- Debit and credit transactions
- c. Pre-set warnings on changes in the balance of current accounts, savings accounts or accounts attached to credit cards:
 - Increase/decrease of the account balance above/below a pre-set threshold;
 - Debiting/crediting of the account with an amount above a pre-set threshold;
- d. Add/Delete/Print out warnings from the phone
- e. Information about the exchange rate of the Bank and the NBR exchange rate of the current date or any earlier date for the following currencies: USD, EUR, GBP, CHF and JPY. The previous date may not be older than one year from the date of requesting the information.
- f General information about the offer of services and products of the Bank.
- g. Any other features that will be launched by the Bank after signing the contract.

2. Technical means necessary to use MyBRD SMS

Using MyBRD SMS involves owning a mobile telephone connected via subscription or prepaid card to the network of one of the Romanian Mobile Telephone Operators licensed for GSM, operating on Romanian territory or in one of the countries with which the operator has roaming agreements (if the Subscriber has enabled the service that allows him/her to use the telephone abroad). In this contract, these operators shall hereinafter be referred to as Telephone Operators.

3. Accounts used to conduct transactions via MyBRD SMS

- a. The Subscriber's Accounts referred to in MyBRD SMS are exclusively the accounts opened with the Bank units. The list of usable accounts and functionalities offered through MyBRD SMS shall be communicated to the Subscriber prior to concluding the contract. The type of accounts accessible via MyBRD SMS shall be modified in time by the Bank, subject to the Client's notification. The Subscriber may subscribe to MyBRD SMS with new accounts by changing the Subscription Application at any of the Bank's units or via the MyBRD Contact Service.
- b. For the accounts used by the Subscriber to join MyBRD SMS the same shall be the Holder or the Proxy only if the account holder is an Individual Client.

4. Access to MyBRD SMS and security requirements

- a. To be able to join MyBRD SMS, the Subscriber shall indicate at least one current account, savings account or account with attached, credit card which may be used via MyBRD SMS, and used as a support account.
- b. Request/receipt of information via MyBRD SMS:
 - Upon request: by SMS order sent to the short dedicated number 1701.
 - Regularly: with periodicity predetermined by the Subscriber (daily, weekly, monthly) for information regarding the balance of current accounts, savings accounts, accounts with attached credit card, loan accounts, deposit accounts and for information on the exchange rate.
 - By generation of pre-set warnings.
- c. The MyBRD SMS service grants the Subscriber the possibility to be informed at any time 24/7 on the situation on the accounts with which the same joined the service.
- d. The access to MyBRD SMS is only possible with the use of the security code (PIN) provided by the Bank at the time of the service activation. This is an alphanumeric randomly generated code and its change by the Subscriber is required for using the service. The PIN code can be written both in lower and in upper case letters. The Subscriber is required to keep the security code as confidential. As

a security measure, the connection with MyBRD SMS is interrupted after the entering of three incorrect PIN codes. PIN resetting can be done at the request of the Subscriber through arrangements made by the Bank and notified to the Subscriber.

5. Responsibilities specific to the MyBRD SMS Service

5.1. For the Bank

- a. To implement the means of receipt and/or issue of computerized data.
- b. For the content of messages as long as they are in the computer system of the Bank.
- c. The Bank is not responsible for:
 - The failure of the telephone due to unpaid telephone bills or the breach any other obligations that the Subscriber has to the mobile telephone operator.
 - The non-receipt of a message by the Subscriber due to the malfunctioning of the mobile phone/operator's network or the fact that it is not in the range of the telephone operator.
 - The loss of integrity of the data transmitted correctly and completely by the Bank, due to the fault of the telecommunications service providers.
 - The failure of sending/receiving of messages on the Subscriber's mobile phone as a result of mobile phone settings made by the latter or of restrictions enabled/required by the telephone operator.
 - The incorrect information entered by the Subscriber from the mobile phone keyboard.

5.2. For the Subscriber

- a. To purchase from own resources, a mobile phone that supports the MyBRD SMS service and to ensure its operation/maintenance and connection to one of the Telephone Operators.
- b. To keep the mobile phone and SIM card safe. The Bank shall not be responsible for transactions made in the event of loss, theft or borrowing thereof.
- c. To immediately call the Telephone Operator to lock the SIM card in case of a loss or theft of the phone and of the SIM card.
- d. To inform the Bank immediately of the occurrence of any event which might prevent the access to messages, especially if the telephone or the SIM card is lost or stolen, of changing the telephone number, of terminating the Contract with the Telephone Operator. In the absence of instructions to the contrary, the Bank shall continue sending messages to the telephone number given in the particular conditions of the Application of Subscription to the MyBRD SMS Service.

6. The monthly usage fee and fees related to transactions

- 6.1. The use of MyBRD SMS service requires the payment by the Client of the following categories of Bank fees:
 - a. The monthly fee for use: it is levied monthly on the 1st of the month, from the support account, for the use of the service in the previous month.
 - b. The fee related to balance query and mini-statement of account for current accounts, savings accounts and accounts with an attached credit card: it is levied from the account for which the information is requested, before sending it.
 - c. The fee for received messages such as: warnings, information on the balance for deposit accounts and loan accounts, queries on the exchange rate, general information – it is levied monthly on the 1st of the month, from the support account, for the messages received in the previous month.
- 6.2. The monthly fee for use, as well as the fees related to transactions and received messages are completely the responsibility of the Subscriber. The amount of the monthly usage fee and the fees related to the transactions via MyBRD SMS are published in the Guide of fees and commissions for Individuals of the Bank and are made available to Subscriber through the Bank

units and the Subscriber states and signs that these lists have been made available and he/she is aware of their content.

6.3 The Subscriber has the option to change the support account of the contract.

6.4 The Bank reserves the right to subsequently alter the fees related to the use of this channel for distribution of banking products and services and undertakes to notify the Subscriber in advance.

6.5 Transactions performed in the accounts used by the Subscriber to join MyBRD SMS and any other related bank fees are reflected in the account statement of the Subscriber.

6.7 At the express request of the Subscriber, the Bank shall provide a detailed list of the transactions.

6.8. The cost of the SMS messages incurred by the Subscriber is the one charged by Telephone Operators and is directly levied by the operator by the monthly invoicing or by direct debiting from the telephone card credit (in case of prepaid cards).

D. MyBRD Net INTERNET BANKING SERVICE (*this section is applicable to clients contracting the service until 26.04.2021*)

MyBRD Net Internet banking service is a “Remote Banking” service accessible from any device with Internet access which offers the following features:

1. Consultative Features

- a. Consulting information on the account balance;
- b. Consulting information on the cards held;
- c. Consulting details on account transactions;
- d. Consulting information on the exchange rate;
- e. Consulting information on the investment funds held by the Client at BRD Asset Management;
- f. Consulting information on the commercial offer of the Bank, including commercial or promotional messages;
- g. Monthly statement of account;
- h. Consulting details on the credit reimbursement schedule;
- i. Consulting information on the pension funds held at BRD Pensii;
- j. Consulting and updating the agreement on the use of personal data by the Bank for marketing purposes, commercial communications, studies, analyses and surveys.
- k. Expressing consent for the provision of account information services through AISP.

2. Transactional Features

- a. Performance of credit transfers between own accounts or for which the Subscriber acts as the Proxy, regardless of the currency in which the accounts are opened; the credit transfers involving foreign exchanges are performed only between the accounts of the same Client;
- b. Performance of intra and inter-bank payments to third party beneficiaries, both in Romania and abroad;
- c. Definition, in the application, by the Subscriber, of third party beneficiaries;
- d. Opening of current accounts and savings accounts;
- e. Opening of term deposits on behalf of the Subscriber, by transfer from the current account;
- f. Liquidation of deposits on their term or before term;
- g. Remote buy and sell fund units for investment funds managed by BRD Asset Management;
- h. Filling in the «Investment profile Evaluation» and «Opportunity Test» surveys;
- i. Signing of the framework agreement on the provision of the reception and transmission of subscription orders and / or redemption of fund units between the Client and the Bank, depending on the availability of MyBRD Net Internet banking service;

j. Making bill payments to the issuers which the Bank provides in the dedicated menu;

k. Subscription to the MyBRD Mobile service;

l. Request of card PIN resetting;

m. Request for issuing a debit card;

n. Manage mobile devices (smartphone, tablet) used to access the MyBRD Mobile banking service through the dedicated app.

o. Expressing consent for the provision of payment initiation services through PISP.

The list of features available to the Subscriber upon signing this Contract may be supplemented by the Bank. These can be used by the Subscriber without being necessary to conclude an addendum to this Contract. If the Subscriber believes that the new features are contrary to his/her interests, he/she may terminate the Contract, under the provisions mentioned in this Contract.

3. The Personal Finance Manager feature

An effective tool of revenue management by lowering costs and boosting savings and investments

For Clients aged 14 to 18, the following functions of the MyBRD Net Internet banking service are available:

- I. Checking of the balance for the account with an attached Sprint and of the Atusprint savings account;
- II. Transfer of funds from the account with an attached card to the Atusprint account.

4. Technical means required to use MyBRD Net Internet banking service

The access to the MyBRD Net Internet banking service can be achieved through any device connected to the Internet and equipped with an operating system and software which are compatible with the security conditions imposed by the Bank to allow accessing www.mybrdnet.ro via the Internet network.

5. Accounts usable by MyBRD Net Internet banking service

- a. The list of accounts usable by MyBRD Net Internet banking service shall be notified to the Subscriber before concluding the Contract on this service and it is also available on the Bank website www.brd.ro;
- b. To be able to join MyBRD Net Internet banking service, the Subscriber shall indicate at least one current account, savings account or revolving account opened with the Bank.
- c. The Subscriber shall indicate upon joining MyBRD Net Internet banking service:
 - The accounts with which he/she shall join the MyBRD Net Internet banking service;
 - The support account from which the costs related to the MyBRD Net Internet banking service will be collected.
- d. The Subscriber's accounts with which he/she joins My BRD Net Internet banking service are exclusively accounts opened with the Bank;
- e. The Subscriber may join MyBRD Net Internet banking service with the accounts for which he/she acts as the Holder or Proxy. The Proxy will no longer have access to the specified accounts in case of revocation of the power of attorney, death of the Holder or if he/she no longer fulfils the conditions of this Contract;
- f. The Subscriber may make additions/suppressions of accounts from the list of accounts within the MyBRD Net Internet banking service directly or by coming to the Bank or by contacting the MyBRD Contact service;
- g. The Subscriber has the option to change the Support Account of the contract;
- h. If the Support Account of the Contract is deleted from the list of accounts that may be accessed by MyBRD Net Internet banking service, the Subscriber will define a new Support

Account. Otherwise, the Contract shall be terminated without any notice.

6. MyBRD Net Internet banking service access and security requirements

- a. To be able to join MyBRD Net Internet banking service, the Subscriber shall indicate at least one active account usable via MyBRD Net Internet banking service;
- b. MyBRD Net Internet banking service access is only possible by using the security elements provided by the Bank at the time of signing the Contract and modified by the Subscriber upon the service activation;
- c. Defining the security elements:
 - *User code*: it is numeric, has eight characters and is used to access the service. The code is communicated to the Subscriber upon joining the service/ signing the contract.
 - *Password*: sent on the main telephone number indicated by the Subscriber; it has six numerical characters. It shall be used both to access the service and sign the transactions performed by it. The user may change this password at any time.
 - *Activation ID*: 6 numerical characters, communicated to the Subscriber by the Bank when activating the MyBRD Mobile application on a device. After activation, this code will no longer be requested to the Subscriber in order to access the application.
 - *One-time password*: sent on the main phone number indicated by the Subscriber; it has six numeric characters. The one-time password is used only with the activation ID upon the first accessing of the mobile token from the MyBRD Mobile application. After enabling the token, the one-time password will no longer be required from the Subscriber to access the application.
 - *Mobile token PIN*: password consisting of six numeric characters defined by the Subscriber upon the first accessing of the mobile token from the MyBRD Mobile application. The PIN shall be used to generate one-time passwords used to sign transactions performed via MyBRD Net Internet banking service. The Subscriber has the possibility to modify the PIN at any time via the PIN change function in the MyBRD Mobile application.
 - *Mobile Token*: authentication software built into the MyBRD Mobile application. It uses a process based on two factors for authentication to ensure system security. The Subscriber enters the PIN code in the Token to access the application and to generate one-time passwords for signing transactions.

or

- *Token Hardware*: a portable device that dynamically calculates passwords based on 3-DES cryptographic algorithm which are valid for a limited period of time. For Token Hardware security, it is in turn provided with a 4-digit PIN code for access which is determined by the user on the first access.
 - *SMS OTP*: a 6-character one-time password sent to the main telephone number indicated by the Subscriber with limited validity which may be used to sign transactions.
- d. Methods of authentication and signing (client profiles):
- *Profile 1*: User code and mobile Token or Token Hardware
 - *Profile 2*: User code, password and mobile Token or Token Hardware
 - *Profile 3*: user code, password and SMS OTP
 - *Profile 4*: user code and password

e. The Subscriber is entirely responsible for maintaining and using the customized Security Features and the consequences of their disclosure or use by third parties.

f. All transactions issued by the Subscriber shall be signed according to the security method chosen to be sent to the Bank.

The Subscriber is responsible for all the consequences resulting from a transmission or handling error on his/her part.

g. As a security measure, the elements of service activation (activation code or one-time password) are blocked after they are entered erroneously five times. New activation elements shall be assigned in this case.

h. As a security measure, the connection with MyBRD Net Internet banking service is interrupted after erroneously entering the Security Features (PIN, Password or user code) five times. In case of forgetting or losing the Security Features, the Subscriber may ask the Bank to assign new Security Features, by contacting the Bank in this regard.

In case of loss/stolen or any unauthorized use of the hardware Token, the Subscriber will notify the Bank as soon as possible to notify the event and cancel the lost Token. In this case, the Bank will replace the token and the new one is obtained by the means provided by the Bank in this regard, subject to bearing the related fee as per the Guide of fees and commissions for individuals.

7. Conditions specific to consultative features

a. The information related to the Subscriber's accounts with which he/she joined MyBRD Net Internet banking service and the transactions in these accounts may be accessed by visiting www.mybrdnet.ro by the Subscriber.

b. The information related to the accounts and transactions performed in it, communicated to the Subscriber via the MyBRD Net service, correspond to the accounting entries made by the Bank at the time of providing the information. This information may be subject to correction and may be made available to Subscribers later, if already initiated and handled transactions are found not to have been accounted for or to have been accounted for incorrectly.

c. The update of the information on the status of the accounts is performed on business days at intervals determined by the Bank. The update of the information is dependent on the type of each credit or debit transaction of the account and the processing thereof.

d. General, economic and financial information provided by the MyBRD Net Internet banking service is informative in nature.

8. Conditions specific to transactional features

a. Credit transfers may only be made from accounts opened with the Bank appearing on the list with which the Subscriber has joined MyBRD Net Internet banking service, in the currency of the debited account.

b. Credit transfers may be made to the accounts featured on the list of beneficiary accounts with which the Subscriber has joined the service at the time of signing the Contract or subsequently joined by the methods provided by the Bank in this regard and presented on the website of www.mybrdnet.ro, and by the beneficiaries defined by the Subscriber in the application (based on their profile). The Subscriber is entirely responsible for the accuracy of the beneficiaries' data manually entered in the application.

c. The rules for processing and performing credit transfers shall be communicated to the Subscriber at the time of signing the contract, and the Subscriber has the obligation to regularly

get informed on them. The Bank does not process transactions that are not conducted in accordance with these rules and is exempted from liability for any damage caused to the Subscriber or third parties involved, due to the non-performance of credit transfers in these cases.

d. Inter-bank payments made by MyBRD Net Internet banking service after the limit time communicated to the Client at the time of signing the Contract shall be processed on the first business day immediately following the date of transmission.

e. Before ordering a credit transfer, the Subscriber shall ensure the existence of sufficient balance in the account that will be debited. In case of insufficient balance in the account of the Subscriber, the Bank reserves the right not to operate the credit transfer and is exempted from liability for any damage caused to the Subscriber or third parties involved.

f. Credit transfers may be performed up to a maximum threshold per transaction and per day. These limits are set by the Bank and may change subject to the prior notice of the Subscriber in accordance with this Contract.

g. The Bank is exempted from liability for any loss or any damage caused to the Subscriber, the payee or any third party involved due to the non-performance of credit transfers if the credit transfers ordered by the Subscriber via MyBRD Net Internet banking service do not comply with this Contract and shall not pay any damages to such party or third any party.

h. The Bank is not responsible for the content of payment orders (e.g. transactions details, beneficiary bank, etc.), it shall take over and send payment orders as they are filled in by the Subscriber. The Bank does not have the right to amend the payment orders signed and sent by the Subscriber to the Bank or to cancel the transaction initiated at the request of the Subscriber under this Contract.

9. Responsibilities specific to MyBRD Net Internet banking Service

9.1. For the Bank:

- a. To implement the means for receiving and issuing computerized data.
- b. The Bank is not responsible for:
 - The downtime of the service or device that enables the connection to the Internet due to any cause not attributable to the Bank.
 - The loss of integrity of the data transmitted correctly and completely by the Bank, due to the fault of telecommunications service providers.
 - Incorrect information entered by the Subscriber in the application, including information of third party beneficiaries.
 - Corruption of transmitted data due to the existence of viruses, spyware or malware installed abusively on the Subscriber's device.
 - Defects or errors arising due to the installation of versions of the operating systems on the Subscriber's device other than those from the list of supported operating systems.

9.2 For the Subscriber:

- a. To order by own means the purchase of the device/software and ensure its connection to the Internet. The Bank is not an Internet, hardware or software material supplier, so it cannot be liable to the Subscriber in this regard.
- b. To ensure, before a credit transfer, the existence of sufficient balance in the account that will be debited. In case of insufficient balance in the account, the Bank reserves the right not to operate the credit transfer and is exempted from liability for any damage caused to the payee Subscriber or any third parties;

- c. The Subscriber is responsible for all consequences resulting from a transmission or handling error on his/her part.

10. Pricing of the MyBRD Net Internet banking Service

a. The service is offered based on a monthly payable management fee, in compliance with the Guide of fees and commissions Individuals.

b. The levying of the monthly usage fee for the MyBRD Net Internet banking service starts in the month following the signing of the Contract regarding the MyBRD Net Internet banking service. The amount of the monthly usage fee is charged in the first five days of each month and refers to the previous month. If the Subscriber does not ensure the availability of an amount sufficient to cover the monthly fee, the access to MyBRD Net Internet banking service will be suspended. It shall be reactivated when it is possible to take the monthly fee from the account. The Bank reserves the rights to terminate the Contract if, within 90 days of the date of suspension, the service is not reactivated.

c. For each transaction made via the use of MyBRD Net Internet banking service, distinct fees and charges shall apply, in compliance with the Guide of fees and commissions Individuals. In order to use the MyBRD Net Internet banking service, the Bank provides the connecting device (Token hardware), for which a purchase fee is charged in accordance with the Guide of fees and commissions for Individuals.

E. MYBRD Mobile - MOBILE BANKING SERVICE

(section applicable to client contracting the service until 26.04.2021)

MyBRD Mobile - Mobile banking service is a "Remote banking" service that can be accessed from any mobile phone (smart phone, tablet, web browser phone or basic mobile phone) that provides both consultative and transaction functions for the accounts with which the Subscriber joined the service and provides the following features:

1. Consultative Features:

- a. Consulting information on the account balance;
- b. Consulting details on account transactions;
- c. Consulting information on the exchange rate and reference interest;
- d. Consulting information on the pension funds held at BRD Pensi;
- e. Consulting information on the investment funds managed by BRD Asset Management held by the Client;
- f. Consulting information on the commercial offer of the Bank, including commercial or promotional messages;
- g. Consulting the list of agencies of the Bank and ATMs of the Bank, using GPS data supplied by the compatible mobile terminals.
- h. Consulting loan offers by means of the loan simulator (informational instrument);
- i. Consulting and update of the agreement on the use of personal data by the Bank for marketing purposes commercial communications, studies, analyses and surveys;
- j. Expression of consent for the provision of account information services through AISP.
- k. Information service on Clients' Bank accounts : advisory-type functionality that allows the user to view accounts held at other banks (including BRD - Société Générale) in a single platform, thus having an overview of the finances and transactions.

Adding Banks by the user (with all accounts and transactions) is done by providing the authentication elements in the Internet Banking service held at the respective Bank. The account types which can be visualized are: current accounts, savings accounts,

deposits, credit accounts, investment funds. For use of this functionality, the user accepts the specific Terms and Conditions, chooses the bank he wants to connect to (from the list of available) and provides the login elements (username/code and password). In case they are not dynamically generated, the authentication items are stored (e.g. static password). In case the authentication implies a second factor (SMS code), this must also be entered. Using these credentials, the user is provided with an overview of the accounts, balances and transactions history. The expenses are grouped by category, according to the Client's option and there is also an option to apply filters to the information displayed, to choose the Bank, account type or currency.

The account data will be updated for each bank, by each user, at the desired moment.

2. Transactional Features:

- a) Operating credit transfers between the accounts with which he/she joined the service or for which the Subscriber acts as proxy, regardless of the currency in which the accounts are denominated; the credit transfers that implies foreign exchange are performed only between the accounts of the same Client;
 - b) Operating payments, intra and interbank, to third party beneficiaries,
 - c) The Subscriber defining, in the application, the third party beneficiaries;
 - d) Opening of current accounts and savings accounts;
 - e) Opening of term deposits on behalf of the Subscriber, by transfer from the current account;
 - f) Liquidation of deposits upon maturity or before the deadline;
 - g) Making payments of invoices to the invoice registers that the Bank shall provide in the dedicated menu;
 - h) Manage mobile devices (smartphone, tablet) used to access the MyBRD Mobile - Mobile banking service through the dedicated app;
 - i) Money transfer through card - the Client may replenish the current account with an amount of money through transfer from debit card issued by another bank in Romania under Visa or Mastercard logo (both accounts must be in the same currency – RON).
 - j) Expression of consent for the provision of payment initiation services through PISP.
 - k) Authorization of payments made online with the card.
- For Clients aged 14 to 18 years, the following functions of MyBRD Mobile banking Service are available:
- I. Consulting the account balance with Sprint card attached and the AtuSprint savings account;
 - II. Transfer of funds from the attached card to the AtuSprint account.

3. Technical means required for using MyBRD Mobile Mobile banking service:

The access to MyBRD Mobile banking service is operated via a terminal device (mobile phone, tablet), regardless of the mobile operator/internet provider or the type of SIM card (prepaid or with subscription).

MyBRD Mobile banking service is available via three channels, depending on the technology used for each type of phone:

Channel 1 (smart phone, tablet): dedicated application for smart phones and tablets using one of the following operating systems:

- Android, version 2.1 minimum. The dedicated application may be downloaded from the Google Play Store;
- iOS, version 4.3 minimum. The dedicated application may be downloaded from the Apple App Store;
- Windows Phone, version 7.5 minimum. The dedicated application may be downloaded from the Windows Phone Store.

Channel 2 (Mobile Web Browser): accessible from any phone that has Mobile Browser by accessing www.mybrdmobile.ro.

Channel 3 (USSD): accessible from classic mobile phones, via USSD session, by calling the dedicated short number.

When using the service on the smart phone, tablet or web browser, the phone is required to be connected to the Internet, regardless of the connection, either through the network of the mobile phone operator or through wireless networks. Connecting to the Internet network is not required for accessing the service via USSD session.

The functions available for each channel depend on the technology used by each phone.

4. Accounts usable via MyBRD Mobile banking service:

- a. The list of accounts usable via MyBRD Mobile banking service shall be notified to the Subscriber before concluding the contract for this service and it is available on the Bank website www.brd.ro;
- b. In order to join MyBRD Mobile banking service, the Subscriber must indicate at least one current account or a revolving account opened with the Bank.
- c. The Subscriber shall indicate, upon joining MyBRD Mobile banking service:
 - The accounts with which he/she shall subscribe to the MyBRD Mobile banking service;
 - The support accounts from which the costs related to the MyBRD Mobile banking service shall be collected.
- d. The accounts of the Subscriber, with which he/she subscribes to MyBRD Mobile banking service are exclusively accounts opened with the Bank;
- e. The Subscriber may join MyBRD Mobile banking service with the accounts for which he/she acts as holder or proxy. The proxy shall no longer have access to the accounts specified in case of revocation of the power of attorney, if the account holder dies or if he/she no longer fulfils the terms of this Contract;
- f. The Subscriber may operate additions/deletions of accounts from the account list within MyBRD Mobile banking service, by coming to the Bank or by contacting the MyBRD Contact service;
- g. The Subscriber has the option to change the support account of the Contract.
- h. If the support account of the Contract is deleted from the list of available accounts for MyBRD Mobile banking service, the Subscriber shall define a new support account. Otherwise, the Contract will be terminated without any prior notice.

5. Access to MyBRD Mobile banking service and security requirements

- a. In order to join MyBRD Mobile banking service, the Subscriber must indicate at least one active account usable via MyBRD Mobile banking service;
- b. The access to MyBRD Mobile banking service is only possible by using the security codes provided by the Bank

at the time of signing the Contract and modified by the Subscriber upon service activation;

c. Defining security features for each channel:

Channel 1: Smart phone/tablets:

- ID or activation code, formed of 6 numerical characters, communicated to the Subscriber by the Bank upon joining the service/signing the contract. The code is used only upon activating the Application on a device. After activation, this code shall no longer be requested from the Subscriber in order to access the application.
- One-time password: sent to the main telephone number indicated by the Subscriber, formed of 6 numerical characters. The one-time password is used only with the activation ID upon the first access to the application. After activation, the one-time password shall no longer be required from the Subscriber in order to access the application.
- PIN: numerical password formed of 6 characters, defined by the Subscriber, upon the first access to the application. The PIN shall be used to sign (authorize) every transaction through MyBRD Mobile banking service. The Subscriber has the possibility to modify at any time the PIN, via the PIN change function within the Application.
- Digital fingerprint. The subscriber can choose this option only after enabling access to the service and registering the fingerprint on the mobile device used. The option is enabled by entering the PIN and can be deactivated at any time by the Subscriber in the MyBRD Mobile Settings menu. This option is available for compatible iOS or Android mobile devices depending on their technical features.
- Mobile Token: authentication software built into the Application. It uses an authentication process based on two factors, in order to ensure system security. The Subscriber introduces the PIN code in the Token in order to access the application and to sign transactions.

Channel 2: Mobile Web Browser

- User code: numerical, formed of 8 characters and used to activate the service. The code is communicated to the Subscriber upon joining the service/signing the contract.
- One-time password: sent to the main telephone number indicated by the Subscriber and formed of 6 numerical characters. The one-time password is used only with the activation ID, upon the first access to the application. After activation, the one-time password shall no longer be required from the Subscriber in order to access the application.
- Cookies: small pieces of data sent from a webpage and stored into the browser of a user while navigating a certain website. When the user returns to said website in the future, the data stored in the cookies are sent back to the website by the browser, in order to notify on the previous activity of the user. If the phone does not allow saving these cookies, this text message will be generated each time the application is accessed from the browser. If the cookies are saved, after activation, this step will no longer be requested to the Subscriber in order to access the application.
- Password: as defined by the Subscriber during the Application activation process. The password shall be requested for accessing the application and for signing transactions. The password must have at least 6 characters and must be numerical.

Channel 3: USSD

- User ID: numerical, formed of 8 characters and used to activate the service. The code is communicated to the Subscriber upon joining the service/signing the contract

- Telephone number: the main telephone number of the Subscriber. This number is the one used for accessing the USSD session.

- PIN: numerical password formed of 6 characters, defined by the Subscriber upon the first access of the application. The PIN shall be used for signing (authorising) every transaction via MyBRD Mobile banking service. The Subscriber has the possibility to modify at any time the PIN, via the PIN change function within the application.

d. The Subscriber is entirely responsible for maintaining and using the customized security elements and for the consequences of their disclosure or use by third parties.

e. All transactions issued by the Subscriber must be signed on the grounds of the method specific to each channel, in order to be sent to the Bank. The Subscriber is responsible for all consequences resulting from a transmission or manipulation error on his/her part.

g. As a security measure, the service activation elements (activation code or one-time password) are blocked after entering them erroneously five times. In this case, it is necessary to assign new activation elements.

h. As a security measure, the connection with MyBRD Mobile banking service is interrupted after entering the Security elements erroneously (PIN, Password or user code) three times. In case of forgetting or losing Security elements, the Subscriber may request the Bank the assignment of new Security elements, by contacting the Bank in this regard.

6. Conditions specific to consultative functions

a. The information related to the Subscriber accounts with which he/she joined MyBRD Mobile banking service and the transactions operated with these accounts may be accessed by the Subscriber by accessing the dedicated application for smart phones/tablets, at the address: www.mybrdmobile.ro for Mobile Web and by calling the dedicated short number for the USSD channel.

b. The information related to the accounts and transactions operated with these, communicated to the Subscriber via MyBRD Mobile banking service, correspond to the accounting entries recorded by the Bank at the time of providing the information. This information may be subject to corrections and may be made available to the Subscriber at a later date, if it is found that already initiated and processed operations were either not recorded or were recorded incorrectly.

c. The update of information on the status of accounts is performed on business days, at an interval established by the Bank. The update of information is dependent on the type of each credit or debit account transaction and the processing thereof.

d. The general, economic and financial data provided by MyBRD Mobile banking service have an informative nature.

7. Conditions specific to transactional functions

a. The credit transfers may be operated only from accounts opened with the Bank and found in the list with which the Subscriber joined MyBRD Mobile banking service, in the currency of the debited account.

b. The credit transfers may be operated to the accounts found in the list of beneficiary accounts with which the Subscriber joined the service at the time of signing the Contract, or to the beneficiaries named by the Subscriber in the application. The Subscriber is entirely responsible for the accuracy of the beneficiary data that he/she manually introduces into the application.

c. The rules for processing and operating credit transfers will be communicated to the Subscriber at the time of signing the contract, as the Subscriber has the obligation to regularly become informed of these. The Bank does not process the transactions that are not operated in accordance with these rules and is exempted from liability for any damage caused to the Subscriber or to third parties involved, due to the non-execution of credit transfers in such cases.

d. The inter-bank payments made by MyBRD Mobile banking service after the deadline communicated to the Client at the time of signing the Contract, shall be processed on the first business day following transmission date.

e. Before ordering a credit transfer, the Subscriber must ensure the existence of a sufficient balance in the account that shall be debited. In case of an insufficient balance (transferred amount and related fee) in the account of the Subscriber, the Bank reserves the right not to operate the credit transfer and is exempted from liability for any damage caused to the Subscriber or to third parties involved.

f. The credit transfers can be performed within a maximum limit per transaction and per day. These limits are set by the Bank and may be changed with the prior notification of the Subscriber in accordance with this Contract.

g. The Bank is exempted from liability for any loss or any damage caused to the Subscriber, the payee or any third party involved, due to the non-execution of credit transfers, if the credit transfers ordered by the Subscriber via MyBRD Mobile banking service do not comply with this Contract, and shall not pay any damages to these parties or to any third party.

h. The Bank is not responsible for the content of payment orders (e.g. transactions details, beneficiary bank, etc.), it shall retrieve and transmit the payment orders as they were filled in by the Subscriber. The Bank does not have the right to modify payment orders signed and sent by the Subscriber to the Bank, nor to cancel the transaction initiated at the request of the Subscriber, under this Contract.

8 Responsibilities specific to the MyBRD Mobile banking service

8.1. For the Bank:

a. To implement the means for receiving and issuing computerized data.

b. The Bank is not responsible for:

- The telephone downtime due to the failure to pay the invoice or the failure to fulfil any obligations the Subscriber has in relation to the mobile telephone operator.

- The loss of integrity of data transmitted correctly and completely by the Bank, due to the fault of telecommunication service providers.

- Incorrect information entered by the Subscriber in the application, including information on third party beneficiaries.

- Phone malfunction due to physical and software failures thereof;
- Corruption of transmitted data due to the existence of viruses, spyware or malware installed abusively on the device of the Subscriber.

- Defects or faults arising due to the installation of versions of operating systems, on the device of the Subscriber, other than those from the list of supported operating systems.

- The impossibility to send/receive data on the mobile phone of the Subscriber as a result of settings performed by the latter or due to restrictions enforced by the telephone operator.

c. The Bank reserves the right to deactivate the Digital fingerprint authentication option in MyBRD Mobile banking service if it encounters security risks for fingerprint scanning technology, in which case it will inform the Subscriber either before deactivation or, if not possible, immediately after disabling the option.

Mobile-specific technology that allows fingerprint scanning is not created by the Bank, so the Bank is not responsible and does not provide any warranty as to the security or operation of this technology.

8.2 For the Subscriber:

a. To order, by own means, the purchase of the mobile phone and ensure its connection to any GSM network and the Internet network. The Bank is not an supplier of Internet connection, GSM networks or hardware or software materials, therefore it cannot be held liable by the Subscriber in this regard.

b. To ensure, before ordering a credit transfer, the existence of a sufficient balance in the account to be debited. In case of an insufficient balance, the Bank reserves the right not to operate the credit transfer and is exempted from liability for any damage caused to the Subscriber, payee or any third party;

c. To immediately call the mobile telephone network operator in order to block the SIM card, in case of theft or loss of the phone and/or SIM card.

d. To keep the mobile device and the SIM card safe. The Bank shall not be held liable for transactions in the event of loss, theft or borrowing thereof. The subscriber must provide security measures to protect the mobile device against unauthorized access by other people and, if opting for the use of the Digital fingerprint, not to save other people's fingerprints in the memory of the mobile device.

e. The Subscriber is liable for all consequences resulting from an own transmission or handling error.

9. MyBRD Mobile banking service pricing

a. The service is provided for a monthly payable management fee, in compliance with the Guide of Fees in RON and foreign currency for individuals.

b. The monthly usage fee for the MyBRD Mobile banking service is charged starting with the month following the signing of the Contract regarding the MyBRD Mobile banking service. The amount of the monthly usage fee is charged in the first five days of each month and refers to the previous month. If the Subscriber does not ensure the availability of an amount sufficient for covering the monthly fee, the MyBRD Mobile banking service access will be suspended. It shall be reactivated when the monthly fee may be collected from the account. The Bank reserves the right to terminate the contract, if the service is not reactivated within 90 days.

c. For each transaction operated via MyBRD Mobile banking service, distinct tariffs and fees shall apply, in compliance with the Guide of fees and commissions for Individuals.

XI. CHANGING /SWITCHING ACCOUNTS SERVICE

Is a service that allows any individual holder of a current account to request the transfer from a Payment Service Provider to another the following:

- (i) either information relating to all or some of the standing orders for credit transfer, recurrent direct debits and recurring incomings through credit transfers, executed in a current account,
- (ii) either the positive balance of the payment account from one payment account to another,
- (iii) either of both (i) and (ii) with or without closing the old account, without the account holder contacting the Bank itself.

The account change service can only be made between payment accounts held in the same currency.

The Bank may act as Recipient Service Provider (New Bank) or Payment Service Provider Performing the Transfer (Previous Bank).

I. Change/switch of account service on the national territory:

If the Bank is the Recipient Payment Service Provider (New Bank), it provides the account change service upon receipt by the Client of the Authorization, completed and signed.

By Authorization, the Client has the possibility to:

a) gives its consent to the previous Bank regarding:

1. transmitting to the new Bank, and, if the Client expressly requests this, to the Client, a list of (i) existing programmed payment orders for credit transfers and (ii) available information on direct debit mandates which are changed;

2. the transmission to the new Bank of the available information on (i) recurring incomings through credit transfer and (ii) the direct debits initiated by the payment payees executed in the account Client's payments in the last 13 months;

3. not accepting direct debits and incomings through credit transfer from the date indicated in the Authorization;

4. cancellation of permanent payment orders from the date indicated in the Authorization;

5. transfer to the payment account opened or held by the Client at the new Bank of any positive balance remaining in the Client's payment account on the date indicated by the Client;

6. closing the payment account

b) to give its consent to the new Bank regarding:

1. establishment of the standing orders for the credit transfers requested by the Client and their execution starting with the date indicated in the Authorization;

2. make any necessary preparations to accept direct debits from the date indicated in the Authorization;

3 informing payers making recurring payments by credit transfer to the Client's payment account as referred to in the Authorization in connection with the details of his payment account held with the new Bank and the transmission to the payer of a copy of the Authorization, out of which to appear clients agreement to change the account;

4.informing the beneficiaries of the payments specified in the Transfer Authorization, using a direct debit facility to collect funds from the Client's payment account, in relation to the details of the Client's payment account with the new Bank and the date from which the direct debits are collected from the respective payment account and sends a copy of the Transfer Authorization to the payees.

c) to clearly identify incomings through credit transfer, standing orders by credit transfer and direct debit mandates to be exchanged;

d) to specify the date from which the standing orders for credit transfers and direct debits must be executed from the payment account opened or held with the new Bank.

If the Bank acts as Payment Service Provider Performing the Transfer (Previous Bank), upon receipt of a request from the new Bank, perform the following operations, if provided in the Authorization:

a) provides the new Bank with a list of existing standing orders for credit transfers and available information on the direct debit mandates that are exchanged;

b) provides the new Bank with the available information on recurring incomings through credit transfer and direct debits

initiated by the creditor, executed in the Client's payment account in the last 13 months;

c) no longer accepts incomings through credit transfer and direct debits from the Client's payment account from the date indicated in the Authorization;

d) cancels the permanent payment orders from the date indicated in the authorization;

e) transfers the positive balance remaining from the Client's payment account to the payment account opened or held by the Client at the new Bank on the date indicated in the Authorization;

f) closes the payment account on the date indicated in the Authorization, except when:

- the Client has outstanding obligations in relation to the payment account in question;

- the current account is used for other services contracted by the Client;

- the account is seized or unavailable, in accordance with the legal provisions, for the Client's fulfilment of obligations assumed to the creditor himself or to third parties.

II. Cross-border account opening facility for clients

If the Client informs the Bank that wishes to open a payment account with a Payment Service Provider located in another Member State of the European Union, upon receipt by the Client of such a request, the Bank shall perform the following types of assistance:

a) provides to the Client, free of charge, a list of all standing orders for active credit transfers at that time and the direct debit mandates generated by the debtor and the available information on recurring incomings through credit transfers and direct debits initiated by the creditor executed on the account of Client's payments in the last 13 months;

b) transfers any remaining positive balance to the payment account held by the Client to the payment account opened or held by the Client with the new Payment Service Provider, with the condition that the request includes full information to identify the new Payment Service Provider and of the Client's payment account;

c) closes the payment account held by the Client, except when:

- the client has outstanding obligations in relation to the payment account in question;

- the current account is used for other services contracted by the Client;

- the account is seized or unavailable, in accordance with the legal provisions, for the Client's fulfilment of obligations assumed to the creditor himself or to third parties.

PACKAGES OF PRODUCTS AND SERVICES SPECIFIC REQUIREMENTS

I. General Principles

1. The packages of products and services offered by the Bank represent groups of products and services having a supportaccount. The products and services included in a package maintain their specific operating conditions.

2. The support account is the current account opened by the Client, through which the operations related to the products and services in the package are carried out. The current account with basic services can be a support account of the package only if the Client waives the fee benefits related to the current account with basic services and accepts the benefits and the other conditions of the package.

3. A package includes a series of products and services that are mandatory for the lifetime of the package, detailed in the specific forms. The failure to meet the conditions for activating any mandatory product (for example, not picking up the card from the Bank by the agreed deadline, etc.) automatically results in the non-activation of the contracted package. In such case, the activated products and/or services will operate individually, according to the product characteristics and will be charged in accordance with the Guide of fees and commissions for Individuals in force on the contracting date.

4. Other products and services provided by the Bank (but not within the Package chosen by the Client) can be attached to the package support account, as individual products under standard pricing conditions - in effect, at the request of the Client.

5. The Bank may provide preferential pricing conditions upon purchasing a package, by comparison to the individual purchase of the products and services. In addition, the Bank may grant preferential pricing conditions to holders of BRD packages, for other products/services provided by the Bank - in which case, the preferential fee conditions will apply for the period of during which the package is held, starting with the first due date of the respective costs, subsequent to acquiring the package.

6. A product/service cannot be simultaneously part of several packages owned by the same Client (except for MyBRD Contact service, MyBRD SMS service, Mobile/internet banking service). Also, the benefits related to the package cannot be cumulated with those related to a salary agreement or other monetary rights.

7. The Client holding the package has access to a number of extra banking benefits, negotiated by the Bank with external partners. The extra banking benefits negotiated by the Bank may undergo changes and shall be periodically updated within the promotional materials and on www.brd.ro.

II. Purchasing a package of products and services

The client can purchase a package of products and services through BRD units, online (if the relationship with the Bank takes place through the institutional website www.brd.ro), as well as through the MyBRD Contact service. In this respect, the Client will fill in the fields corresponding to the packages and the options related to the products included in the package, in the specific form provided by the Bank, in hardcopy or in electronic format, as the case may be. In case of contracting the package through the MyBRD Contact service, the necessary information and the Client's options will be collected during the telephone interaction with the Bank and will be confirmed by the Client by e-mail. The contract/package subscription application, along with:

- the General Banking Conditions for individuals;
- the Guide of fees and commissions for individuals;
- the List of interest rates charged by BRD; and
- the Contracts specific to the products and services included in the package, as well as their annexes, represent the contract specific to the package.

III. Fees

Throughout the existence of the package, the Client owes and will pay to the Bank the commissions and costs related to the package of products and services, according to the following mentions below. They are automatically deducted, at maturity, from the package support account or, if there are not sufficient funds available in the

package support account, from any other customer account. These fees are as follows:

a. The package management fee, which includes:

- the support account administration fee;
- the debit card administration fee included in the package;
- the subscription for remote banking services and the free operations included in the package.

The package management fee is charged as follows:

a1) For current account packages with the condition of receiving recurring income:

- if the recurring income condition is met, the monthly package administration fee is 0 (zero) for the month in which this condition is met;

- for each month in which the condition of recurring income is not fulfilled, the package administration fee is charged on the 20th day of the following month;

a2) For current account packages without the condition of receiving recurring income: on a monthly basis, on the day corresponding to the day of purchasing the package);

b. The annual Comfort insurance premium. In case of inclusion in the package of an insurance contracted before the package, the preferential premium will be taken from the next annual maturity date.

IV. Changing the structure of the packages of products and services

1. The Bank has the right to modify the structure of the packages of products and services already contracted by the Client, by removing/replacing certain products from the package, if they are no longer part of the Bank's offer. Any change in the structure of the product and service packages will be notified to the Client and will enter into force on the date mentioned in the respective notification.

V. Changing the held package of products and services with another package

In order to change the held package of products and services with another package existing in the Bank offer, the Client shall terminate the old package and shall request the opening of a new one.

The products and services included in the old package:

- will be included in the new package, if they are included in its structure. The bank will transfer them from one package to another under the fee conditions specific to the new package; or, as the case may be
- will be passed on the standard fee conditions, in force at the date of closing the package, if they are not included in the structure of the new package. The client has the opportunity to close these products and services in accordance with the functionalities and provisions characteristic of each product/service.

VI. Terminating the package of products and services

1. Each Contracting Party shall have the right to unilaterally terminate the Contract that covers the package of products and services with a 30 calendar days notice, communicated in writing to the other party.

2. Upon the termination of the package, the Client may:

- Waive all the products from the package of products and services;

- Keep one, several or all products included in the package as stand-alone products (if available in the Bank offer and individually, outside the packages). In such case, for all the products and services that the Client keeps, the standard commissions and interests of the Bank, in force at the time of closing the package, will become applicable.

3. The contract regarding the package of products and services will be terminated, by unilateral termination by the Client, only on the condition of the termination of all due and unpaid payment obligations arising from the respective contract.

4. The Bank may terminate the package of products/services or any product/service related to it in case of non-payment of commissions/costs related to the package and/or products included in it and/or in case of non-compliance by the Client with any contractual obligations.

VII. Closure of the products and services within the package

1. A product/service included in the package may be closed:

a. by the Client, upon request;

b. by the Bank, under the provisions of this contract.

2. The closure of products and services included in the package may result in the closure of the respective package or not, as follows:

a. The closure of optional products/services which are part of the package does not imply the closure of the package. The following are optional products/services included in the package:

- Remote banking services: Mobile and internet banking services, MyBRD SMS service, MyBRD Contact Center service (in case these services are optional in the package, according to the specific forms), CONFORT Insurance, BRDAV Hospitalization Insurance and possible extra banking services that may be contracted on the grounds of the subscription to the package of products and services. After terminating such products/services, the package shall continue to operate. The Bank shall continue to charge package management fee from its support account, at the same level as at the date of the contract.

b. The closure of mandatory products/services included in the package implies the termination of the package. The following are mandatory products/services included in the package:

- The support account (current account or paid current account);

- The cards attached to the support account, purchased within the package of products and services, including the cards renewed/issued but not collected from the banking unit within the agreed period.

- Remote banking services: MyBRD Contact service, MyBRD SMS service, the internet and mobile banking services (only if the services are mandatory in the package), according to the documentation for opening each package).

As a result of the closure of one of the mandatory products that generate the closure of the package, the products and/or services included in the package structure will function individually according to the product features and will be charged in accordance with the Guide of fees and commissions for Individuals into force at the package closing date, starting from the next maturity date.

ANNEX. Information Note on the Processing of Personal Data²

B.R.D. - Groupe Société Générale S.A., headquartered in Bucharest, Blvd. Ion Mihalache, No. 1-7, Sector 1, registered with the Trade Register under number J/40/608/19.02.1991, Tax Identification Number 361579, registered with the Banks Register under number RB-PJR-40-007/1999 (hereinafter called „The Bank” or „Us/ We”), in the capacity of personal data operator, we would like to inform you about the way We process³ the personal data in the context of the activity carried out by BRD, as well as about the rights that you have as a data subject, starting with 25th of May 2018 (GDPR effective date).

I. WHAT DATA CATEGORIES DO WE PROCESS?

By case, the Bank processes the following personal data categories:

- **identification data**, such as name, surname, CNP, ID card serial and number/other document which can serve as identification (e.g. passport, residence permit), as well as other information these documents may contain (e.g. date and place of birth, citizenship, gender: masculine/ female, type of ID card, issuing date, expiring date), signature, personal data contained in the digital certificate if you use the electronic signature in the relationship with the Bank.
- **marital status**, such as data from the marriage certificate.
- **contact data**, such as: home address, mailing address, e-mail, phone number.
- **video or static image**, if entering into relationship with the Bank and/or contracting certain products and services does not imply your physical presence in our units or when you visit the Bank’s offices or you use the Bank’s ATMs. Our surveillance system does not capture by focusing, selective targeting or profiling but only by continuously or sequentially processed recordings with low or high definition quality.
- **voice**, if entering into relationship with the Bank and/or contracting certain products and services does not imply your physical presence in our units and in the case of calls registration to achieve the purpose D „Services - support and complaint management” under point III „Why do we process personal data?”
- **data necessary for the evaluation of your eligibility**, such as:
 - information regarding your professional qualifications, such as information regarding your occupation, employer’s name, position, etc.
 - „know your Client” information, such as your public function, political exposure, special relations with the BRD Groupe, etc.
 - fiscal information, such as country/ countries of fiscal residence and fiscal identification number;
 - information regarding your financial-economical status, such as income, solvability, credit history, assets owned in property.
 - transactional information (such as transactional history, type of product: deposits, savings accounts, etc., opening/maturity date, initial or current amounts/balances, including outstanding

amounts, seized amounts, etc.).

- information regarding fraudulent activities or, where applicable, potentially fraudulent, such as accusations and convictions for (attempted) fraud, misdemeanors or criminal offences (for money laundering and/or financing terrorist acts).
- data regarding the guarantees (information regarding the initial owners of the property brought as collateral);
- health data contained in: documentation specific to loans granted to cover medical expenses, such as: data contained in documents issued by the health institution certifying the level of costs related to treatment/ hospitalisation/ investigations/ intervention; and/or in documents issued by the General Directorate for Social Assistance and Child Protection (Direcția Generală de Asistență Socială și Protecția Copilului), in case of loans for the purchase of vehicles adapted for people with disabilities and/or in the case of loans for adapting of houses according to the individual access needs of persons.
 - **any other data, necessary or useful for the Bank’s activity**, as per the law, as well as personal data that are disclosed by data subjects in various circumstances related to interactions with the Bank.

Note: In case of clients represented by agents/ other forms of representation, the Bank will process the personal data of the person who represents the client (such as name and surname, date and place of birth, personal identification number or a similar identifier, home address and its legal regime – such as domicile, residency, citizenship), including other personal data mentioned in the document certifying the power of representation.

II. WHERE DO WE HAVE THE PERSONAL DATA FROM?

We process the personal data that you provide Us, directly or indirectly (e.g. through empowered or other persons representing you in your relationship with the Bank, such as, persons who are entrusted with the exercise of parental/ tutorial authority), or that data that We generate or deduct as a result of the interaction with you through any of the channels of communication with the Bank. We can also obtain and process your personal data including from external sources, such as:

- **public institutions and authorities** (e.g. ANAF, FNGCIMM, NBR - Credit Risk Center or Payment Incidents Center (CIP), National Integrity Agency, National Pension House, etc.). For example, We can interrogate the databases of authorities/ public institutions to obtain certain information, such as: your tax situation, including your fiscal identification number, the Declaration of Wealth, in the case of politically exposed persons; ; the status of your forced execution file; your employee status; information on the status of the claim file by the FNGCIMM; your identification data in the Credit Risk Center, including information on the type of loan contracted, the degree of indebtedness and the affiliation to a group of debtors.
- **registries and electronic databases** (e.g. Courts portal, the Credit Bureau, National Register for Movable Assets, entities empowered

² Implemented in accordance with the provisions of Regulation (UE) 2016/679 of the European Parliament and of the Council of April 27, 2016 on the protection of natural persons with regard to the processing of personal data and of the free movement of such data, and repealing Directive 95/46/CE („GDPR” - General Data Protection Regulation - regulation for protecting personal data), applicable starting with May 25, 2018.

³ The data processing designates any type of operation (collection, storage, copying, deletion, disclosure, etc.) that targets personal data (data that can lead Us to you or to another individual person).

to manage databases with designated persons, subject to international money-laundering sanctions and politically exposed persons, etc.). For example, but not limited to, when entering into relationship with the Bank, We interrogate (i) the Court's portals to verify if you are involved in criminal litigations likely to reveal a certain fraudulent conduct, (ii) the Credit Bureau, to check the Bank's exposure by reference to your payment behaviour or other incidents in relation with other banks, in case you request a credit product from our Bank (iii) if you are included in databases with designated individuals, subject to international sanctions that block the funds.

- **entities involved in payment operations** (e.g. international cards organizations, such as Visa and Mastercard, economic operators accepting cards payments, banks and other payment institutions involved in payment schemes, the Central Depository). For example, when you make transactions with the card, We can receive some data necessary to make the payments (e.g. the card's data, transaction amounts) from merchants who accepted the payment with the card. Also, in other types of operations (e.g. credit card payment, direct debit, debit instruments such as cheque, promissory note), We can receive your data from a bank/ third-party institution where the transaction was initiated, through schemes/ payment systems and interbank communications (such as SEPA, Regis, SENT or SWIFT).
- **commercial partners**, in particular service providers for the Bank. For example, We may find out your new contact information (e.g. address, phone number) from agencies providing debt recovery services for Us, data that they obtain from their own sources.
- **health institutions**: clinic/hospital, state/private, General Directorate for Social Assistance and Child Protection (Direcția Generală de Asistență Socială și Protecția Copilului), any other institution providing medical treatment/subsidising the repayment of loans to people with disabilities, etc.
- **online platforms** (social media and internet) publicly available, including data aggregators.
- **entities in BRD Group** (such as data on clients who had contracts with BRD Finance IFN S.A).
- **your employers**, for example if We enter into a payroll agreement with your employer.
- **other companies for which the Bank provides payment services** (securities issuers, insurance companies, etc.).
- **certificate issuers**, if you use the electronic signature;
- **Central Depository**, as a registry company for the Bank's shares.

For example, in certain situations, We may obtain your personal data from Bank's clients/ Bank's clients' Client representatives (e.g. if you are a member of the Client's family), board members of the Bank (if you are an affiliated person), if such data are necessary in the context of legal relations with the Bank's client.

The refusal to provide the Bank with your personal data may, in some cases, result in the impossibility of entering into relationship with the Bank or of contracting the desired product, service.

III. WHY DO WE PROCESS PERSONAL DATA?

A. ENTERING INTO RELATIONSHIP WITH THE BANK

We process personal data for:

- a) Checking your eligibility for entering into relationship with Us and contracting the banking product/ service, as well as for
- b) Preparing the required documentation for contracting the product/ service.

We check your situation to ensure that you meet the prudential requirements, under the applicable law and internal policies of the Bank (including the risk policies). For example: We apply „know your Client” procedures, for which we process data such as: your name, surname, date and place of birth, ID type and country of issuance, personal identification number, ID series and number,

home/ residence address, fiscal identification number, telephone number, fax number, e-mail address, citizenship, multiple citizenship if applicable, source of funds, activity area, occupation and workplace, purpose and nature of the relationship with the bank, declared income range, politically exposed person/ member of the family of a politically exposed person or a close associate of a politically exposed person, public function, etc; We verify that you meet the requirements concerning the fraud prevention and combating money laundering and terrorist financing; We evaluate your situation as well as, if applicable, of other persons (e.g. co-debtors, guarantors) to analyze the Bank's exposure to the risk involved by contracting the required banking product/ service.

For certain products (such as loan products), We also use automated processing (including scoring) to assess your eligibility for contracting the product (for details, please see Section IV below).

Processing basis:

Entry into the contractual relationship, including the processing carried out at your request for the conclusion and performance of the contract. In case it is necessary to process special categories of personal data (e.g. health data) in order to conclude the contract with you, we will ask for your explicit consent.

BRD's legitimate interest to check its clients' Client eligibility in terms of internal policies and standards imposed at BRD Group/ Société Générale Group level.

Compliance with legal obligations.

Note: In case of clients represented by agents/ other forms of representation, the Bank will process, in order to identify the agent / other representative, his / her identification data, as mentioned in section I above, as well as other personal data, if needed, in order to assess the power of representation.

B. PROVIDING BANKING PRODUCTS AND SERVICES. PRODUCTS AND SERVICES MANAGEMENT

We process personal data to conclude and execute the contract with you. To prevent and combat fraud and/ or guarantee the banking secrecy: We verify the authenticity of identity documents as well as, if the case, of other documents that you submit; We monitor the way the contract is performed and the associated risks; We apply procedures for managing conflicts of interest.

We may contact you or, as the case may be, other persons (such as co-debtors, guarantors, agents, legal representatives) through various channels (e.g. phone, e-mail, SMS, at home), to communicate you/ them various aspects concerning the contract or the contracted banking product/ service.

For example, if difficulties arise in executing the contract, We may contact you to identify together the optimal solutions to continue the contractual relationship with you in the best possible conditions. We may also send you notifications regarding payment maturities or concerning changes in the features of the contracted banking product/ service.

Processing basis:

Entry into the contractual relationship and performance of the contract.

Compliance with legal obligations.

BRD's legitimate interest to ensure the contracts performance in an optimal and efficient manner.

C. ECONOMIC, FINANCIAL AND ADMINISTRATIVE MANAGEMENT. ANALYSES AND INVESTIGATIONS FOR INTERNAL USE

We use personal data to optimally organize and streamline the Bank's activity. In this regard, We may use personal data, among others:

- to organize some internal databases, to support the activity carried out by structures and departments within the Bank.
- to improve and optimize BRD's network activity, as well as our processes, products and services.
- to efficiently organize, perform and/ or manage debt collection and debt recovery.
- to prevent and investigate possible fraud/ fraud suspicions in banking operations.
- to perform various financial analyses, in an aggregated format, regarding the performance of BRD's network and its staff (including the Bank's sales force).
- to prepare various reports, in an aggregated format, on (a) BRD's activity and performance in financial and banking markets, and (b) its exposure to other financial institutions.
- to support Our position in various investigations, administrative and judicial procedures, litigations, etc. in which the Banks is involved.
- in the context of various analyses, internal audit procedures and/ or investigations carried out by the Bank, on its own initiative or following the receipt of a complaint from a third party (including public authorities).
- managing controls/ investigations triggered by public authorities.
- for the development and testing of IT applications and systems, used to provide services to Clients as well as to support the Bank's activity;
- to ensure the security of information systems;
- for archiving, both in paper form and in electronic format of documents, as well as backing up electronic data.

Processing basis:

BRD's legitimate interest to streamline and optimize its activity.

D. SUPPORT - SERVICES AND COMPLAINTS MANAGEMENT

We process your personal data to solve your requests or of other persons, as well as for providing you/ them with additional information about our products and services.

For example, We may contact you by phone to respond to your requests or We may process certain data from the documents you provide Us with to solve your requests or complaints (such as a request to update your data or to block the card).

We audio record the conversations with you in order to improve the quality of our services as well as to test (a) your requests/ claims concerning a particular banking product/ service as well as, eventually, our response, respectively (b) your agreement/ option/ preferences for a particular product or service of ours. If you do not want to record the conversations above mentioned, you can contact Us on other available channels, such as by e-mail or by writing Us to our dedicate contact address. In this latter case, the effective settlement of your request/ complaint will not be affected in any way, but the settlement may be longer.

Processing basis:

Contract conclusion and execution, including for processing at your request for concluding the contract.

Compliance with specific legal obligations.

BRD's legitimate interests (i) to comply with a legal obligation and to avoid any negative consequences, and (ii) to carry out its activity in accordance with internal standards and with the standards established at the Group level.

The data subject's consent - you can withdraw your consent at any time - for details, please see Section VIII d) below.

E. DIRECT MARKETING AND COMMERCIAL COMMUNICATIONS

We want to keep you updated with the latest news about the products

and services of the Bank and/ or of other companies within Société Générale (such as insurance companies, pension funds, leasing companies, investment funds etc.) and/or of our partners (such as insurance companies outside Société Générale Group) , to invite you to participate in contests or advertising lotteries that We organize on our own or with our partners (co-organizers). Before contacting you, We may also consider our internal analyses and studies (for details, please see Section H below).

In line with the aforesaid, We may also send you commercial communications, including direct marketing messages (selling of products and services) regarding the aforementioned products/ services.

We will only send you direct marketing messages and other commercial communications if We have obtained your consent.

F. SURVEYS AND MARKET RESEARCH

We are interested in your opinion about our products and services, about Us or other companies within the Group in general or about a particular subject relevant to our activity. We can periodically contact you to receive your feedback and suggestions on how to improve our products and services or how we can better meet your needs and expectations. You are not obliged to respond and if you do not respond, it will not affect in any way your relationship with Us.

We also carry out market studies; for this purpose , We can work with market research agencies, which will either conduct market studies for Us, or provide us with market research results and other information related to the subject of such studies. Usually, we receive information regarding the market studies from our partners in anonymised format (aggregated data).

Also, if you do not exercise your right to object, We may use your physical address to transmit you by courier or by post commercial communications (leaflets, catalogs, etc) with news about our products and services, invitations to participate in contests or advertising lotteries that We organize on our own or with our partners.

Processing basis:

BRD's legitimate interest.

Your consent - you can withdraw your consent at any time - for details, please see Section VIII d) below.

G. OFFERS/ PRODUCTS PERSONALISATION

We want to offer you the most relevant products and services according to your profile and area of interest. Therefore, based on your agreement, We may analyze your data and information from the following sources:

- Our internal database, such as information from loan records/ other similar documents that We hold as a result of your previous loan requests/ other products and/ or banking services. For example, We are interested in knowing relevant information in order to evaluate your particular situation such as seniority in relationship with the Bank, age, occupation, income (including as a result of a credit application previously submitted by you), the quality of politically exposed person, the quality in the shareholding structure of a legal entity, the products and services held and their degree of use on different channels (e.g. Internet or mobile banking), the analysis of the typology of the transactions you made within a certain time/per product (e.g. cards)/ per type of traders and the value of the aforesaid transactions,; and/ or
- External sources, such as companies from BRD Group or our partners, international card payment companies, the Trade Registry, Credit Bureau, ANAF.

Offer personalization will not exclude your access to our products and services.

We analyse and combine the data and information mentioned above to provide you the products and services that best fit your needs and particularities. We may also use the aforesaid information to avoid sending you offers for products and services that, for various reasons (including our risk policy), are not of interest to you or you would not be able to access them, due to your particular situation.

The algorithms we apply for offer personalisation are based on information such as: seniority in relationship with the bank, age, occupation, income (including as a result of a credit application previously submitted by you), your previous credit application score, the quality of politically exposed person, the quality of shareholder/ associate in a legal entity, the equipment rate with products and services and their degree of use on different channels (Internet and/ or mobile banking), the analysis of typology and the value of your transactions within a certain time interval/ per product type or by traders. All this information is analysed for determining a statistical model, having as result a tailored product and services offer for you. This offer takes into account your transactional profile and behaviour (as evidenced by the aforementioned information) and will include personalised products and services based on your needs.

The algorithms used may vary over time, so for more information about the logic used in creating offers/ products, you can contact us at the data mentioned in the "**CONTACT**" section.

Sometimes, in the process of offers/ products personalization, we use automated individual decisions.

We can assure you of the adequate guarantees for the automated decisions we make.

You have the right to: (i) express your point of view on that automated decision; (ii) To request a reassessment of the decision, on the basis of a human intervention; (iii) to contest the automated decision.

We will be able to use customized individual decisions to send you personalized offers if We have obtained your **explicit consent** in this respect.

Processing basis:

Your consent - you can withdraw your consent at any time - for details, please see Section VIII d) below.

H. ANALYSES AND OTHER INTERNAL STUDIES

We are preoccupied with the constant improvement of our products and services. Based on our legitimate interest, We use the data that we collect from you or other data that we generate/ deduct from the data received from you (such as: age, based on your CNP) for various statistics, analyses and internal studies.

Most internal analyses and internal studies are in anonymous format (aggregated data), providing Us with useful information for improving our products and services. Sometimes, We analyze your data to determine your specific Client profile, to better meet your needs and expectations.

CLIENT PORTFOLIO SEGMENTATION

We use information such as age, occupation, income (including as a result of a credit application previously submitted by you), the quality of politically exposed person, the quality of shareholder/ associate in a legal entity, the amounts held at the bank and/ or the outstanding of the loans granted by the Bank, in order to classify you into a specific generic profile, determined in accordance with the internal rules for Client portfolio classification.

In the same time, We have a legitimate interest in analyzing your data so as not to disturb you with information that does not fit your profile. For example, We can exclude you from a particular campaign if you

exceed the age that We target for a specific product (such as cards dedicated to students).

We will send you direct marketing messages and commercial communications related to the products designed for the client segment you are part of only if We have obtained your **explicit consent** in this respect.

Processing basis:

BRD's legitimate interest.

Your consent - you can withdraw your consent at any time - for details, please see Section VIII d) below.

I. COMPLIANCE WITH LEGAL REQUIREMENTS AND INTERNAL NORMS

We process personal data also for complying with the legal obligations applicable to credit institutions. For example, based on our legal obligations, We submit various reports to relevant institutions and public authorities, such as: (i) reporting of persons subject to FATCA/CRS to ANAF, (ii) reporting suspicious transactions to the National Office for the Prevention and Control of Money Laundering (ONPCSB), (iii) reporting payment incidents to the Payment Incidents Center (CIP) within the National Bank of Romania, (iv) notifying ANAF within the Ministry of Economy and Finance or as the case may be, notifying other competent authorities when identifying persons or designated entities, (v) Reporting of persons to "Oficiul pentru Implementarea Sanctiunilor Internationale" (MAE), in case of identifying sanctioned persons or entities. We also monitor our Clients' transactions to identify unusual/ suspicious money laundering or terrorist financing transactions, and to prevent fraud, (vi) daily reports to ANAF regarding the Central Electronic Register of Bank Accounts and Payment Accounts, (vii) reporting based on ANAF requests for information and documents, (viii) obtaining the Fiscal Identification Number from ANAF for non-resident clients holding an account or a safe deposit box, in case you do not already have a Fiscal Identification Number or you do not communicate it to Us when opening an account and/or renting a safe deposit box.

According to the law, We cannot initiate a business relationship and will not be able to continue an existing relationship if We are unable to apply know your customer measures.

We also inform You that it is an offence for the Bank to breach its reporting obligations.

Such monitoring may be based on profiling mechanisms and automated decision-making processes, including artificial intelligence-based models, and may involve analysis of transactional behaviour against data collected about you. Profiling mechanisms and automated decision-making processes may involve comparisons with the expected transactional profile of the customer based on information provided to the Bank at the time of relationship initiation/data update for „know-your-customer” purposes. These profiling mechanisms are periodically reviewed to ensure that they remain effective and undistorted.

The processing of data specific to “know-your-customer processes” also includes the processing of data of third parties such as trustee/guardian/guarantor, information which is added to the risk score of the client for which the aforementioned guaranteed.

Considering our membership of the Société Générale Group, exchanges of information with entities in the Group may be realised, exchanges of information aimed at ensuring compliance with legal provisions relating to customer knowledge and the fight against money laundering, thus having public interest considerations.

For some processing within the scope of this purpose (such as: establishing the data necessary for the anti-money laundering analysis, validating the quality of the data before the specific anti-money laundering process is carried out, creating the model

identifying potential atypical transactions to be analysed by Us in order to determine whether they can be considered as suspicious from preventing and combating money laundering perspective, complying with the regulatory obligations in terms of identification and reporting of suspicious transactions), Société Générale SA acts as an associated operator together with Us. Upon request to either of the two operators, you may receive a copy of/ details of the agreement concluded between BRD and Société Générale regarding the processing of your personal data. In essence, BRD will only collect and provide Société Générale with personal data in relation to which it has informed you in advance. To the extent that you submit a request to exercise a right referred to the below Chapter . IX Contact, to either BRD or Société Générale, they will inform and support each other so as to reply to you within the legal time limit (as a rule, one month). As a rule, however, your main point of contact is BRD. In the event of personal data protection incidents requiring your prior information, you will be informed by either BRD or Société Générale.

For additional information concerning the reporting made under our legal obligations, you can request this information.

We can also process your data. for the establishment and management of garnishments, the provision of information on garnished amounts to enforcement bodies or authorities, in accordance with the Bank's legal obligations.

Also, in order to comply with the legal provisions in force, We process personal data through security systems (closed circuit television and visitor's management/ access control) or access record registers, the data being kept for intervals regulated by the law. The data collected under the legislation on the protection of persons, goods and values may be made available exclusively to the authorities, at their request, respecting the conditions provided by the law.

In addition to the legal obligations, We are also committed to complying with a number of internal requirements/ established at the Société Générale Group's level on reporting and internal/ external audit that may, in some cases, involve/ have as a source the processing of personal data.

Processing basis:

Compliance with specific legal obligations.

Carrying out measures in the public interest, in particular to implement the provisions of Law 129/2019 and Regulation 2/2019, as amended.

BRD's legitimate interest and of Société Générale Group to carry out its activity according to internal standards and those established at the Group level.

J. DIVIDENDS PAYMENT TO BRD SHAREHOLDERS

Processing basis: Compliance with specific legal obligations.

K. TO ENSURE THE SECURITY AND PROTECTION OF PERSONS, PREMISES, BANK PROPERTY/ ASSETS AND TO PREVENT AND COMBAT THE VIOLATION OF LEGAL PROVISIONS AND/ OR THE COMMISSION OF CRIMES

We use closed-circuit television ("CCTV") systems to ensure the security and protection of the Bank's premises/assets and persons, for the prevention of crimes.

Access to video recordings is only carried out in situations that justify such processing, such as the occurrence of security incidents, indications of possible unlawful activities by certain persons,

complaints received from other persons reporting certain unauthorized activities captured by the video cameras.

Processing basis:

Compliance with specific legal obligations. for situations where legislation requires video surveillance, such as access areas, ATMs, perimeter of cash processing centres, public work area.

BRD's legitimate interest to adequately manage the security of the Bank's premises and assets as well as persons.

L. FOR THE PREVENTION AND INVESTIGATION OF FRAUD OR OTHER INCIDENTS RELATED TO CASH OPERATIONS CARRIED OUT THROUGH THE BANK'S EQUIPMENT (ATMS, ROBO, ETC.) OR AT THE COUNTER.

We retain images of cash transactions (e.g. time of receipt/deposit of cash at ATMs, etc.) carried out through the machines or at the Bank's cash desks in order to analyse them in case data subjects complain about the non-disbursement of all or part of the withdrawn amounts, the deposit of amounts other than those appearing on the deposit documents, etc.

Processing basis:

The Bank's legitimate interest in protecting itself against fraud or events that may cause damage to both the Bank and the data subjects and to use the images and recordings captured by CCTV systems to administer as evidence during any investigation.

M. FOR THE HANDLING OF COMPLAINTS/ COMPLAINTS RECEIVED FROM DATA SUBJECTS WHERE THE ISSUES RAISED REQUIRE ACCESS TO VIDEO FOOTAGE.

We may analyse the images captured by CCTV equipment for the resolution of complaints/complaints received from data subjects, where appropriate.

Processing basis:

The Bank's legitimate interest (to resolve complaints/ complaints received in a timely manner, as well as to protect against events that may adversely affect the Bank's image, to administer the images captured as evidence during possible investigations, inquiries or lawsuits.

IV. AUTOMATED INDIVIDUAL DECISIONS

Sometimes, in our processes We use automated individual decisions, including as a result of creating profiles, which under certain circumstances may have legal effects or, as the case may be, may significantly affect you. In this case, the automated decisions will always be based on one of the legal bases provided by Article 22 GDPR, namely (i) the need to conclude the contract; (ii) the legal authorization; or (iii) the explicit consent of the data subject. Thus, We adopt automated individual decisions by virtue of a legal authorization, including the implementation of public interest measures required in the areas of customer due diligence, prevention and combating money laundering and terrorist financing. For example, the law requires Us to implement appropriate know your client measures for the purpose of preventing and combating money laundering and terrorist financing.

To this end, We check whether you are included in the databases of persons accused of terrorist financing or economic crime or, as the case may be, in the databases of people with high risk of fraud.

We also use profiling mechanisms/automated decision-making processes to ensure continuous monitoring of the client portfolio and client transactions from the perspective of prevention of money laundering and terrorist financing/implementation of international sanctions. Such mechanisms/processes may use data collected about you in the know-your-customer process, or data from public sources/data aggregators, and may also rely on artificial intelligence-based models. If, following individual analysis, we consider that your profile exceeds the level of risk accepted by the Bank, we will refuse to enter into a relationship with you or the existing relationship will be subject to restrictions or unilaterally terminated.

The use of automated decision-making processes for the purposes of customer due diligence, preventing and combating money laundering and terrorist financing reduces the risk of human error and discrimination, allowing banking services to be provided in accordance with the law, without blocking the enrolment/transaction management process, and allowing adequate collection and reporting of customer and transaction information, as required by law.

For certain banking products, We use automated individual decisions based on scoring to **conclude the contract** for the product you requested. For example, We use the loan scoring to assess your eligibility for contracting the requested loan. The algorithms that We use for the loan scoring consider different criteria, in line with our risk policy, such as your financial condition, your creditworthiness, exposure, payment behaviour, employer status, debt history, etc.

The criteria and the algorithms that We consider relevant may vary over time.

We use automated individual decisions also for ensuring the security of the Bank's products and services, as well as to protect you as much as possible against the risk of fraud, thereby ensuring the proper execution of the contract concluded with you.

For example, We monitor the payments you make online or with your card, and if We identify suspicious transactions (such as unusual repetitive payments like frequency, value, etc., or other transactions with illogical sequences - such as payments in different locations (cities) at short intervals, which did not allow the holder to move to those locations in accordance with the current technique) and/or do not match to your transactional profile, We adopt measures on automated basis (such as blocking the suspicious transaction, blocking the card, blocking the account, etc.). Also, if We have obtained your express consent in this regard, We may use automated individual decisions to transmit you (We or companied within BRD Group, depending on your option) personalized commercial communications (for details, please see Section III G, above).

You will have appropriate guarantees for the automated decisions We take. In particular, you will have the right: (i) to express your point of view on that particular automated decision; (ii) to request a reassessment of the decision, based on human intervention; respectively (iii) to challenge the automated decision.

V. TO WHOM DO WE DISCLOSE PERSONAL DATA?

We may disclose personal data to:

- a) Our **main service providers**, such as:
 - interbank payment processing and payment information transmission services through schemes/ payment systems and interbank communications (e.g. SWIFT - Society for Worldwide Interbank Financial Telecommunication, STFD Transfond S.A. and NBR for ReGIS and SENT national payment systems);
 - services provided by international cards organizations (e.g. MasterCard, Visa etc);
 - services provided by payment service providers;
 - services provided by transaction reporting providers to competent authorities or other regulated entities (e.g. Deutsche Boerse, DTCC);

- cards issuance and personalization services;
 - debt recovery and/ or debt collection services;
 - goods and other assets valuation services;
 - services of capital investment agents/ brokers.
- b) **Marketing services providers**, such as:
 - Marketing agencies;
 - Market research and surveys agencies;
 - Marketing communication agencies (e.g. e-mailing commercial offers);
 - Partners specialised in organizing lotteries and contests.
 - c) Our **support-services and/ or auxiliaries providers**, such as:
 - electronic communication services (e.g. e-mailing, SMS etc.);
 - real estate agencies;
 - bailiffs;
 - IT services (e.g. maintenance, support, development);
 - audit services;
 - physical and/ or electronic archiving services;
 - courier services;
 - legal, notarial or other consulting services;
 - d) **Public institutions and authorities** in Romania and abroad, such as:
 - National Bank of Romania (NBR);
 - Financial Supervisory Authority (ASF);
 - The National Supervisory Authority for Personal Data Processing (ANSDP);
 - National Office for Preventing and Combating Money Laundering (ONPCSB);
 - Oficiul pentru Implementarea Sanctiunilor Internationale (MAE)
 - National Agency for Fiscal Administration (ANAF);
 - Competition Council;
 - National Archives;
 - Courts and other judicial bodies (such as police offices, prosecutor's offices, The National Anticorruption Directorate - DNA etc.);
 - The Bank Deposit Guarantee Fund, The National Credit Guarantee Fund for Small and Medium Enterprises (FNGCIMM);
 - Deutsche Boerse Approved Reporting Mechanism (ARM).
 - e) Certain **Clients of the Bank** with whom you have contractual or legal relationships related to the banking products We provide, such as:
 - Utility services providers (water, electricity, telephony, internet, etc.), for direct debit conventions;
 - Companies with whom you have working relationships and have concluded a payroll convention with Us.
 - f) **Other partners** of the Bank, such as Credit Bureau (including the transmission of data regarding late payments), other financial-banking institutions (for example, correspondent banks and other financial-banking entities participating in schemes/ payment systems and interbank communications such as SEPA, ReGIS, SENT, SWIFT), The National Pension House (in the case of pension rights payments through a bank account opened with Us), The Central Depository, pensions and/ or insurance companies, insurance brokers/ damage assessors, investment fund management companies providing for Us or, as the case may be, for which We provide various services, other entities (such as banks or banking-financial institutions) in connection with the sales or restructuring operations of debts portfolios and/or other rights of the Bank based on the legal relations established with you.
 - g) Société Générale Paris, entities from the **Société Générale Group and BRD Group**, such as Société Générale Global Solution Centre India (SG GSC INDIA) and Société Générale Global Solution Centre Romania (SG GSC ROMANIA), under the terms of the law. To check out the complete Group

VI. DATA TRANSFER ABROAD

As a rule, We transfer personal data only in states belonging to the European Economic Area (EEA) or states that been recognized as having an appropriate level by a decision of the European Commission.

We may, however, transfer personal data to other countries than those listed above if:

- a) The transfer is made **on the basis of appropriate guarantees** (such as, through the use of Standard Contractual Clauses issued by the European Commission or adopted by the competent authority, together with, where appropriate, additional protective measures about which we can inform you upon request or by using other clauses - subject to their approval by the competent authority or the applicable Corporate Rules at BRD level);
- b) The transfer is performed based on certain international treaties between the European Union and the third country (e.g. agreements between the EU and the US);
- c) The transfer is **necessary to execute the contract** with you, for example if you want to transfer an amount of money from your account to a bank account located in a third country, We have to disclose your personal data in order to execute the requested bank transaction.

Note: *In order to be able to make a funds transfer abroad, the banks (including the Bank) uses the settlement services offered by SWIFT.*

SWIFT temporarily stores SWIFT transaction data on servers located in the E.U., but also in the USA. Under applicable SWIFT legislation, it may be required to disclose to the US authorities data stored on US servers for money laundering prevention and fight against terrorist financing activities.

- d) Other cases allowed by the law.

We may also transfer your personal data to other SG Group entities for various purposes as per **Section III. Why we process personal data (mainly point I) and V. To whom we disclose your personal data.**

We mention that the data processed through CCTV systems are not transferred abroad.

VII. FOR HOW LONG DO WE KEEP YOUR DATA?

We keep your personal data as long as necessary to meet the purposes for which it was collected, in compliance with the applicable legal provisions, as well as of the internal procedures on data retention (including the applicable archiving rules at BRD level).

For example, if you are our client, We will keep your personal data, as a rule, throughout your contractual relationship with Us, with an additional period of at least 10 years.

If we will not enter into a banking relationship with you, your data collected during the initiation of pre-contractual arrangements will be retained for a period of 5 years.

Note: For customers represented by the agents/ other forms of representation, the bank will process the agent's / representative's data for the purposes set out in section III A above, according to the retention terms applicable to the documents relating to the operation covered by the mandate.

Upon request, you can obtain additional information regarding the retention periods applicable to your personal data.

In case of processing carried out by means of surveillance cameras, we keep your data for a period of at least 20 days but not more than 30 calendar days. In exceptional situations, in case of incidents or the defence of any legal interest/right, we keep your personal data for as long as necessary for their investigation, i.e. until the conclusion of the legal proceedings in compliance with the applicable legal provisions on the matter, as well as internal procedures on data retention.

VIII. WHAT ARE THE RIGHTS THAT YOU BENEFIT FROM?

According to the Law, you benefit from the following rights concerning the personal data processing that We perform:

- a) **Right of access to personal data:** you may obtain from Us the confirmation that We process your personal data, as well as information regarding the specific nature of the processing, such as: the scope/ the purpose, the categories of personal data processed, the recipients of the data, the period for which the data are kept, the existence of the right to rectification, erasure or restriction of the processing. This right allows you to obtain a copy of the processed personal data, as well as any extra copies for a fee.
- b) **Right to rectification:** you may ask Us to modify your incorrect personal data or, if the case, to fill in the data that is incomplete.
- c) **Right to erasure:** you may request the erasure of your personal data when: (i) the data are no longer necessary for the purposes for which We have collected and processed them; (ii) you have withdrawn your consent for processing your personal data and We can not process it for any other legal ground; (iii) the personal data are unlawfully processed, respectively (iv) the personal data have to be erased for compliance with the relevant legislation.
- d) **Consent withdrawal:** you may, at any time, withdraw your consent regarding the processing of your personal data, data processed on a consent basis.
- e) **Right to object:** you may object, at any time, to the processing of personal data for marketing purposes, including profiling for the same purpose and you may also object to processing based on Bank's legitimate interest, for reasons related to your specific situation.
- f) **Right to restriction of processing:** you may request to restrict the processing of your personal data if: (i) you dispute the accuracy of the personal data, for a period enabling Us to verify the accuracy of the personal data; (ii) the processing is unlawful and you oppose the erasure of the personal data and request the restriction of their use instead; (iii) the data is no longer needed for the purposes of processing, but you require them for exercise or defence of legal claims; respectively (iv) if you have objected to processing, for the period of time during which it is verified whether the legitimate rights of the Bank as an operator prevail over your rights as a data subject.
- g) **Right to data portability:** to the extent that We process personal data by automated means, you may request, under the Law, to provide you with your personal data **that you have provided** in a structured, commonly used and machine-readable format (e.g. CSV format). If you request this, We can send your personal data to another entity, if possible from a technical point of view.
- h) **Rights related to automated decisions that We adopt in our business:** for details, please see Section IV above.
- i) **Right to file a complaint with the Supervisory Authority:** you have the right to file a complaint with the Supervisory Authority if you consider that your rights have been violated:

National Supervisory Authority for Personal Data Processing	Bld. G-ral. Gheorghe Magheru 28-30 Sector 1, postal code 010336 Bucharest, Romania anspdcp@dataprotection.ro
--	--

Note: The right of access personal data, the right to rectification, the right to erasure, the right to restriction of processing, the right to object and the right to file a complaint with the National Supervisory Authority for Processing of Personal Data are also applicable to agent's/ representative's data, in case of clients represented by agents/ other forms of representation.

FOR EXERCISING THE ABOVE-MENTIONED RIGHTS, ITEMS a) - h), YOU MAY CONTACT US USING THE CONTACT DATA REFERRED TO IN SECTION VIII (CONTACT).

IX. CONTACT

If you have any questions about this information note or if you want to exercise your rights as a data subject, you may contact Us using the following contact details:

In the attention of: BRD Data Protection Officer (DPO)

Correspondence address:

**Blvd. Ion Mihalache, No. 1-7, Sector 1, BRD Tower,
postal code 011171, Bucharest, Romania**

E-mail: dataprotection@brd.ro

This **Information Note on the Processing of Personal Data** replaces (i) its previous versions and (ii) any contrary provision existing in contracts, forms and/or documents specific to products and services contracted by the client and, where appropriate, completes them.

In the case of clients represented by agents/other forms of representation, the Agent/Legal Representative shall inform the Client that he/she represents of the existence and content of this 'Information on the Processing of Personal Data', as well as of the fact that this document is available free of charge in BRD units and on the Bank's website, in the section <https://www.brd.ro/en/processing-personal-data>.

This information shall be supplemented, in the event of entering into a business relationship with the Bank/contracting a product in the online environment, with specific information on the processing of data made available to the data subject within the respective flows.