BRD

GROUPE SOCIETE GENERALE

NOTIFICATION ON THE PROCESSING OF PERSONAL DATA[1]

B.R.D. - Groupe Société Générale S.A. ("the Bank" or "we"), as the controller, would like to inform you about how we process your personal data[2] in the context of BRD's activity, as well as about your rights as a data subject.

I. WHAT DATA CATEGORIES DO WE PROCESS?

As the case may be, the Bank processes the following personal data categories:

- **identification data,** such as name, surname, personal identification code, series and number of ID card/birth certificate/other identification document (e.g. passport, residence permit, etc.), as well as other information contained therein (e.g. date and place of birth, citizenship, gender, type of identity document, date of issue, expiry date, etc.), signature, personal data included in the digital certificate in case you use electronic signature in your relationship with the Bank, the data from the document (birth certificate/judicial decision) certifying the status of legal representative of the minor/person deprived of legal capacity/person with limited legal capacity.
- **marital status data**, such as marriage certificate data.
- **contact details** such as: home address, mailing address, email, phone.
- **video or static image,** if entering into a relationship with the Bank and/or contracting certain products and services does not imply your physical presence in our premises or when you visit the Bank premises or use our ATMs. Our surveillance system has no right to capture by focusing, selective targeting or profiling, but only by continuously or sequentially processed recordings, at low or high-definition quality.
- **voice**, if entering into the relationship with the Bank and/or contracting certain products and services does not imply your physical presence in our premises and in the case of recording calls for the achievement of purpose D "Services – support and complaint management" under item III "Why do we process personal data?" below and when participating, in order to carry out the contract with you, at conferences/video-conferences in which you have chosen to record the session and you have given your consent for the recording of your voice and the other data communicated during that conference.
- **data needed to assess your eligibility**, such as:

- professional qualification information, such as information on the occupation, the name of the employer, the position held, etc.;
- information serving customer knowledge, such as the public position held, political exposure, special relationships with the BRD Group, etc.;
- tax information, such as country/countries of tax residence and tax identification number;
- information about your economic and financial status, such as income, solvency, credit history, property owned;
- transactional information (such as transactional history, product type: deposits, savings accounts, etc., date of granting/maturity, initial or current amounts/balances, including outstanding amounts, amounts held, etc.);
- information relating to fraudulent or, as the case may be, potentially fraudulent activities, such as charges and convictions for (attempts to) fraud, committing contraventions or offenses (for money laundering and/or terrorist financing, etc.);
- information regarding the warranty, as well as information about the initial owners of the property brought as collateral;
- health data included in: specific documentation for loans intended for covering medical expenses, such as: data included in documents issued by the healthcare institution certifying the level of costs related to treatment/hospitalization/investigations/interventions; and/or in documents issued by the General Directorate for Social Assistance and Child Protection, in the case of loans for the purchase of vehicles adapted for people with disabilities and/or in the case of loans for adapting housing according to the specific individual access needs of people with disabilities;

- **any other data needed or useful for the performance of the Bank's activity**, under the law, as well as personal data made known by the data subjects under various circumstances related to the interactions with the Bank.

Note: In the case of clients represented by the agents/other forms of representation, the Bank will also process the identification data of the person representing the client (such as name and surname, date and place of birth, personal identification code or similar identifier, the address at which they lives and their legal status - such as domicile, residence, citizenship), including other personal data mentioned in the document attesting the power of representation.

II. WHERE DO WE GET THE PERSONAL DATA FROM?

We process personal data that you provide to us, directly or indirectly (for example, through a proxy or other persons representing you in your relations with the Bank, such as persons who are invested with the exercise of parental authority/guardianship), or that we generate or deduct as a result of our interaction with you through any of the communication channels with the Bank.

We can also obtain and process your personal data from external sources, such as:

-**public institutions and authorities** (for example: ANAF, FNGCIMM, NBR - Credit Risk Centre or Payment Incidents Centre (CIP), National Integrity Agency, National Pension House, etc.). For example, we can query the databases of public authorities/institutions to obtain certain information, such as: your tax situation, including Tax Identification Number; statement of assets, in the case of publicly exposed persons; the status of your forced execution file; your status as an employee; information regarding the compensation file by FNGCIMM; your identification details from the Credit Risk Centre, including information on the

[1] Prepared in accordance with the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC ("GDPR"), applicable from 25 May 2018.

[2] Data processing refers to any type of operation (collection, storage, copying, deletion, disclosure, etc.) concerning personal data (data that can lead Us to you or another identified individual).

type of the contracted credit, the level of indebtedness, and membership in a group of debtors.

- **electronic registers and databases** (e.g. courts portal, Credit Bureau, National Register of Movable Property Publicity (RNPM), entities empowered to manage databases with designated persons, subject to international sanctions for blocking funds and those exposed politically, etc.). For example, but not limited to, when entering into a relationship with the Bank, we check (i) the court instances portal to verify if you are involved in criminal lawsuits, likely to reveal a certain fraudulent conduct, (ii) the Credit Bureau, to assess the Bank's exposure related to your payment behaviour or other incidents with other banks, in case you request a credit product, (iii) if you are listed in the databases of designated persons, subject to international sanctions for blocking funds.

-entities involved in payment operations (for instance: international card organizations, such as Visa and Mastercard, economic operators accepting card payments, Banks, and other payment institutions involved in payment schemes, Central Depository). For instance, when you make card transactions, we may receive some data needed to make the payments (e.g. the card data, the amounts related to the transactions) from the traders who accepted the card payment. Also, within other types of operations (e.g. credit transfer, direct debit, cheque payment instruments, bills of exchange, promissory note), we may receive your data from a third-party bank/payment institution where the transaction was initiated, through interbank payment and communication schemes/systems (such as SEPA, Regis, SENT or SWIFT).

- **commercial partners**, particularly service providers for the Bank. For example, we may find out your new contact details. (e.g. address, phone number) from the agencies performing debt recovery services for us, data that the latter obtain from own sources.

- health institutions: clinic/hospital, public/ private, General Protection of Social Assistance and Child Protection, any other institution that offers medical treatments/subsidizes the reimbursement of loans granted to persons with disabilities, etc.

- **online platforms**, (social media and Internet) publicly available, including data aggregators.

- **entities in the BRD Group** (such as data on Clients who have had contracts with BRD Finance IFN S.A).

- **your employers**, e.g. if we conclude a salary payment convention with your employer.

- **other companies for which the Bank provides payment services** (issuers of securities, insurance companies, etc.)

- **issuers of certificates**, if you use an 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 the Bank's clients/representatives of the Bank's clients (e.g. if you are a member of the client's family), members of the Bank's management bodies (if you are a related person), if this data is necessary in the context of legal relations with the Bank's client.

The refusal to provide to the Bank certain personal data may, in certain situations, result in the impossibility to enter into a relationship with the Bank or to contract the desired product or service.

III. WHY DO WE PROCESS PERSONAL DATA?

A. ENTERING INTO A RELATIONSHIP WITH THE BANK

We process personal data to:

a) Verify your eligibility for entering into a relationship with us and for contracting the banking product/service as well as to

b) Prepare the necessary documentation for contracting the banking product/service.

We check your situation to ensure that you meet the prudential requirements, in accordance with the applicable law and the Bank's internal policies (including risk). For example: we apply customer due diligence procedures, in connection with which we process data such as: your first name, last name, date and place of birth, type and country of issuance of identification document, personal identification number, identification document series and number, home address / residence, fiscal residence and tax identification number, phone number, fax, email address, citizenship, multiple citizenship if applicable, source of funds, sector of activity, occupation and place of work, purpose and nature of the relationship with the bank, declared income range, status as a politically exposed person / family member of a politically exposed person or known close associate of a politically exposed person, public function, etc. We verify if you meet the requirements in the field of fraud prevention and anti-money laundering and terrorist financing; we assess your situation, as well as, if applicable, that of other persons (such as co-debtors, guarantors) to analyse the Bank's exposure to the risk involved in contracting the banking product/service you desire.

For certain products (such as credit products), we also use automated processing (including scoring) to assess your eligibility for contracting the product (see for details Section IV below).

Note: In the case of clients represented by agents/other forms of representation, the Bank will process, for the purpose of identifying the agent/representative, their identification data, as mentioned in Section I above, as well as other personal data, as the case may be, for the purpose of verifying the power of representation.

B. PROVISION OF FINANCIAL AND BANKING PRODUCTS AND SERVICES. PRODUCT AND SERVICE MANAGEMENT

We process personal data for the conclusion and performance of the contract with you. To prevent and combat fraud and/or guarantee bank secrecy: we check the authenticity of identity documents, as well as, if applicable, other documents you submit to us; we monitor the way the contract is carried out and the associated risks; we apply procedures for managing conflicts of interest.

We may contact you or, as the case may be, contact other persons (such as co-debtors, guarantors, agents, legal representatives), through various channels (e.g. telephone, e-mail, SMS, at home), to communicate to you/them various aspects related to the contract status or the contracted banking product/service. For example, if difficulties arise in the performance of the contract, we may contact you to identify together the best solutions to continue the contractual relationship with you in the best possible conditions. We may also send you notifications regarding the maturity of payment terms or the occurrence of changes in the characteristics of the contracted banking product/service.

For the execution of payment operations initiated by you or in cases where you are the beneficiary, Transfond SA (the Administrator and the operator of the automated Clearing House for Interbank payments in RON) will have access to the following personal data in order to process a payment for which the settlement is made through Transfond: The IBAN, the beneficiary's name and surname, the amount transferred, the payment details, the payer's name and surname. This information is processed on a contractual basis for the execution of the payment transaction.

The data transferred by us to Transfond SA are accessed by the other participants in the payment scheme administered by Transfond under conditions of legal security and according to strict technical rules. The full list of participants can be found at: https://www.transfond.ro/pdf/Lista%20b%C4%83ncilor%20care%20ofer%C4%83%20SANB.pdf.

In the case of payment services in relation to which we will specifically inform you prior to their implementation, we may act

as joint controllers with Transfond SA. An example of this is the provision of the RoPayP2P service in proximity, a service for initiating instant payment requests by the payment beneficiary user, provided to users by the Participants in the RoPay Scheme (the list of Participants is available on the Transfond website at: https://www.transfond.ro/servicii/casa-de-compensare-automata-sent), in accordance with the set of rules regarding the RoPay Scheme, issued by TRANSFOND SA. BRD is a participant in the RoPay Scheme. We also act as an joint controller with Transfond in order to provide the SANB service described in letter. L below.
When we act as joint controllers with Transfond, if you address a request for the exercise of a right referred to in Section VIII below to any of BRD and Transfond unit, we will inform and support each other so that we can respond to you within the legal period (as a rule, one month). As a rule, your main point of contact is us (BRD), at the address in the "IX. Contact" section below, and if you address Transfond, it will redirect to us your request to exercise your rights provided by the GDPR.
In the event of personal data protection incidents that require your prior information, you will be informed, as a good practice, by us and we will agree with Transfond the content of the information in advance. More information on the processing of personal data carried out by Transfond, including the contact details of the data controller, can be found at: https://www.transfond.ro/contact.

In order to carry out the contract with you, we process your data for the archiving and storage of e-mail correspondence.

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 other things:

- to organize internal databases, as support for the activity carried out by the structures and departments within the Bank.
- to improve and optimize the activity of the BRD network, as well as our processes, products and services.
- to organize, perform and/or manage effectively the debt collection and debt recovery activity.
- to prevent and investigate possible fraud/suspicions of fraud in banking operations.
- to carry out various financial analyses, in aggregate format, on the performance of the BRD network and its staff (including the sales force of the Bank).
- to prepare various reports, in aggregate format, on (a) the activity and performance of BRD in financial and banking markets and (b) its exposure to other financial institutions.
- to support our position in various investigations, administrative and judicial proceedings, litigations, etc. in which the Bank 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).
- to manage of 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.
- to archive documents in both paper and electronic format, as well as for backing up electronic data.

D. SUPPORTING SERVICES AND COMPLAINT MANAGEMENT

We process personal data in order to handle your or other persons' requests, as well as to provide you with additional information about our products and services. By way of example, we can contact you by phone to respond to your requests or we can process certain data from the documents you provide to solve your requests or complaints (such as a request to update data or block the card).
We perform audio recordings of the talks with you to improve the quality of our services, as well as to demonstrate (a) your requests/complaints regarding a certain banking product/service, as well as, potentially, our answer, respectively (b) your consent/option/preferences for one of our products or services. If you do not wish to have the talk recorded as above, you can contact us using other available channels, such as by email or by writing us at our contact address. In this latter case, the actual settlement of your request/complaint will not be affected in any way; however, the settlement period may be longer.

E. COMPLIANCE WITH THE LEGAL REQUIREMENTS AND INTERNAL RULES

We also process personal data to comply with legal obligations applicable to credit institutions. We collect and process your identification data or other data from independent sources, such as public or private databases, including public exposure information, to ensure that the legal provisions relating to customer knowledge and anti-money laundering are met. Also, based on the legal obligations binding us, we submit various reports to the relevant public institutions, such as: (i) reporting on individuals subject to FATCA and/or CRS to the National Agency for Fiscal Administration (ANAF), (ii) reporting suspicious transactions to the National Office for the Prevention and Combating of Money Laundering (ONPCSB), (iii) reporting payment incidents to the Payment Incidents Centre (CIP) within the National Bank of Romania, (iv) notifying the National Agency for Fiscal Administration within the Ministry of Economy and Finance, or as the case may be, other competent authorities, in case of identifying designated persons or entities, (v) reporting individuals to the Office for the Implementation of International Sanctions, in case of identifying sanctioned persons or entities. We also monitor the transactions of our clients to identify unusual/suspicious transactions of money laundering or terrorist financing, and to prevent fraud, vi) daily reports to ANAF regarding the Central Electronic Register of Banking Accounts and Payment Accounts, vii) reports following requests received from ANAF for information and documents, viii) obtaining the tax identification number from ANAF for non-resident account holders or the securities box, if they do not already hold a tax identification number and do not provide it to the Bank at the time of requesting the opening of an account and/or the rental of 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 cannot apply customer knowledge measures.
At the same time, we inform you that the violation of the reporting obligations represents a violation for the bank.
These monitoring activities can be carried out on the basis of automated profiling and decision-making processes, including artificial intelligence models, and may involve the analysis of transactional behaviour compared to the data collected about you. Profiling mechanisms and automated decision-making processes may involve comparisons with the client's expected transactional profile based on the information provided to the Bank at the time of the initiation of the relationship/updating of data for the purpose of customer knowledge. These profiling mechanisms are regularly reviewed to ensure that they remain effective and undistorted.

The processing of data specific to the customer knowledge processes also includes the processing of data of third parties such as the agent/guardian/legal representative/guarantor, the information

regarding them being added to the risk score of the client for whom they endorse/guarantee.

Considering our affiliation with the Société Générale Group, information exchanges can be carried out with entities within the Group, exchanges aimed at ensuring compliance with legal provisions regarding customer knowledge and anti-money laundering, thus having considerations of public interest.

For certain processing within 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 to identify potential atypical transactions that must be analysed by us to determine whether they can be considered as suspicious in terms of preventing and combating money laundering, compliance with regulatory obligations in relation to the identification and reporting of suspicious transactions), Société Générale SA acts as a joint operator with us. At the request of either of the two operators, you may receive a copy of/details of the agreement concluded between BRD and Société Générale with regard to the processing of your personal data. Basically, BRD will only collect and provide Société Générale with personal data regarding which you have been informed in advance. To the extent that you submit a request for the exercise of a right referred to in Chapter. VIII Contact below to any of the BRD and **Société Générale**, they will inform and support each other so that they answer to you within the legal deadline (as a rule, one month). Typically, your main point of contact is BRD.

For the purpose of managing managerial supervision activities and performing internal control regarding all banking operations carried out at BRD, we may process your data to verify compliance with legal requirements, identify and remediate any operational and/or other types of risks.

For the purpose of managing operational risks, we may process your personal data to comply with legal obligations regarding the management of exposure to operational risk/the mitigation of reputational or financial risks, as well as for the smooth running of processes at the Bank level.

In the event of personal data protection incidents that require your prior information, you will be informed by any of BRD and Société Générale. For further information on reports made under our legal obligations, you can request this information from us.

Furthermore, we can process your personal data for the establishment and management of garnishments, providing information regarding the seized amounts to enforcement authorities or entities, in accordance with the Bank's legal obligations.

Also in view of complying with the legal provisions in force, we process personal data through the security systems (closed-circuit television and visitor management/access control) or access records, the data being retained for the legally-regulated intervals. The data collected based on the law on the protection of persons, goods, and valuables may only be made available to the authorities, at the latter's request, in compliance with the conditions provided by the law.

In addition to our legal obligations, we are also required to comply with a number of internal/established requirements of the Société Générale Group regarding the performance of internal/external reports and audits which, in certain situations, may involve/have as source the processing of personal data.

F. PAYMENT OF DIVIDENDS TO BRD SHAREHOLDERS

G. TO ENSURE THE SECURITY AND PROTECTION OF PERSONS, PREMISES, ASSETS/VALUES OF THE BANK AND TO PREVENT AND COMBAT THE VIOLATION OF LEGAL PROVISIONS AND/OR THE CRIMINAL OFFENCES

We use closed circuit television ("CCTV") systems to ensure the security and protection of the premises/assets of the Bank and of persons, in order to prevent crimes.

Access to video recordings shall be made only in situations justifying such processing, such as the occurrence of security incidents, indications of possible illicit activities by some persons, complaints received from other persons signalling the conduct of certain illegal activities caught by video cameras.

H. TO PREVENT AND INVESTIGATE FRAUD OR OTHER INCIDENTS RELATED TO CASH OPERATIONS CARRIED OUT THROUGH THE BANK'S EQUIPMENT (ATMs, ROBO, ETC.) OR AT THE BANK COUNTER.

We retain images of operations in cash (e.g. the time of receipt/deposit of the cash at the automatic teller machines etc.) performed using the equipment or at the Bank's cashier's offices to analyse them if the data subjects claim that the amounts withdrawn were not released in whole or in part, depositing amounts other than those recorded on the deposit documents etc.

We process together with Transfond SA, as a joint operator, your personal data (first name, last name initial, and IBAN code) to provide the Beneficiary Name Display Service (SANB) for electronic payments made to accounts opened at a financial institution in Romania that has joined the SANB, with the aim of preventing fraud in payment operations and unwarranted payments. The data transferred by us to Transfond SA is stored by Transfond SA and updated periodically until the termination of your relationship with BRD and may be queried by the other participants in SANB in the context described above. The full list of SANB participants is found at https://www.transfond.ro/pdf/Lista%20b%C4%83ncilor%20care%20ofer%C4%83%20SANB.pdf.

I. FOR HANDLING COMPLAINTS AND/OR REFERRALS RECEIVED FROM DATA SUBJECTS IN CASE THE ISSUES NOTIFIED REQUIRE ACCESS TO VIDEO IMAGES.

We can analyse the images captured by CCTV equipment in order to settle the complaints received from the data subjects if this is necessary.

You can consult information on the grounds underlying the above-mentioned processing, as well as information on how long we keep your data, within the framework document governing the processing of your data in the context of the relationship with the Bank. This is available on the BRD website, accessible here*https://www.brd.ro/prelucrarea-datelor-cu-caracter-personal.*

The respective framework document supplements this Notice regarding the processing of personal data for purposes such as:

- direct marketing, commercial communications, and personalization of offers/products (in which cases we will process your personal data only if you give us your consent in this regard)
- conducting surveys, market research, analyses, and other internal studies, internal segmentation of the client portfolio (in which cases we will process your personal data based on the Bank's legitimate interest, unless you object to such processing).

IV. AUTOMATED INDIVIDUAL DECISIONS

Sometimes, in our processes, we use automated individual decisions, including as a result of profiling, which, in certain circumstances, may cause legal effects or, as the case may be, may significantly affect you. In this case, automated decisions will always rely on one of the legal grounds provided under Article 22 GDPR, namely (i) the need to enter into the contract; (ii) legal authorisation; or (iii) the data subject's explicit consent.

Thus, we adopt automated individual decisions **by virtue of a legal authorization,** including the implementation of public interest measures imposed in the field of customer knowledge, prevention and combating money laundering and terrorist financing. For

instance, the law requires us to implement adequate Know Your Customer measures for the purpose of preventing and controlling money laundering and the financing of terrorism. For this purpose, we check whether you are included in the data bases of persons accused of terrorist financing or economic crimes, as the case may be, of persons with high fraud risk.

We also use profiling mechanisms/automated decision-making processes to ensure continuous monitoring of the clients' portfolio and transactions made by them from the perspective of preventing money laundering and financing terrorist acts/implementing international sanctions. Such mechanisms/processes may use the data collected about you in the customer knowledge process, or data from public sources/data aggregators, and may also be based on models based on artificial intelligence. If, following the individual analysis, we believe 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 unilateral termination. The use of automated decision-making processes for the purpose of conducting the customer knowledge activity, preventing and combating money laundering and terrorist financing reduces the risk of human error and discrimination, allowing the provision of banking services under the law, without blocking the process of enrolling/managing transactions and allowing adequate collection and reporting of information on clients and transactions, according to legal requirements.

For certain banking products, we use automated scoring decisions to be able to **conclude the contract** for the product you requested. For example, we use credit scoring to assess your eligibility to contract the requested credit. The algorithms we use for credit scoring take into account various criteria in accordance with our risk policy, such as your financial status, creditworthiness, exposure degree, payment behaviour, employer situation, debt history, etc. **The criteria and algorithms that we consider relevant may vary over time.**

We also use automated decisions to ensure the security of the Bank's products and services, as well as to protect you as much as possible against the risk of fraud, thus ensuring **the proper execution of the contract** with you. For example, we monitor payments that you make online or by card and, if we identify suspicious transactions (such as unusual repetitive payments in frequency, value, etc.) or other transactions with illogical sequences - such as payments from different locations (cities) at short intervals that did not allow for the holder to move to those locations according to the current state of technology) and/or that do not correspond to your transactional profile, we take appropriate measures automatically (such as blocking the suspicious transaction, blocking the card, blocking the account etc.)

Also, if we have obtained from you **explicit consent** in this regard, we may use automated individual decisions to send you (we or the companies of the BRD Group, depending on your choice) personalized commercial communications (see, for details, Section IIIG above).

You will benefit from appropriate safeguards for the automated decisions we make. In particular, you will have the right to: (i) express your views on that automated decision; (ii) request a reassessment of the decision based on human intervention; and (iii) challenge the automated decision.

V. TO WHOM DO WE DISCLOSE THE PERSONAL DATA?

We can disclose personal data to:

a) Our **main service** providers, such as:

- interbank payment processing services and transmission of information on payment transactions through payment and interbank communication schemes/systems (e.g. SWIFT - Society for Worldwide Interbank Financial Telecommunication, STFD Transfond S.A. and NBR for the national payment systems ReGIS and SENT);
- The beneficiary name display service (Transfond SA and SANB scheme participants). The list of participants can be found at: https://www.transfond.ro/pdf/Lista%20b%C4%83ncilor%20care%20ofer%C4%83%20SANB.pdf. In the context of payment services administered by Transfond, State institutions and authorities with supervisory and control prerogatives, such as the National Bank of Romania (BNR), may have access to your personal data.
- RoPay service (Transfond SA and RoPay scheme participants. The list of participants can be found at: https://www.transfond.ro/servicii/casa-de-compensare-automata-sent). In the context of payment services administered by Transfond, State institutions and authorities with supervisory and control prerogatives, such as the National Bank of Romania (BNR), may have access to your personal data.
- services offered by international card organisations (e.g. MasterCard, Visa etc);
- services provided by payment processing service providers;
- services offered by transaction reporting providers to competent authorities or other regulated entities (e.g. Deutsche Boerse, DTCC);
- banking card issuing and personalization services;
- debt recovery and/or collection services;
- valuation services for goods and other assets;
- services of investment agents/brokers on capital markets.

b) Providers of **marketing services**, such as:

- Marketing agencies;
- Market research and analysis agencies;
- Marketing communication transmission agencies (e.g. e-mailing commercial offers);
- Partners specialized in organizing lotteries and contests.

c) Our **support and/or ancillary services** providers, such as:

- electronic communication services (e.g. emailing, SMS etc.);
- real estate agents;
- enforcement agents;
- IT services (e.g. maintenance, support, development);
- audit services;
- storage and archiving services in physical and/or electronic format;
- courier services;
- legal, notarial or other consultancy services.

d) **Public institutions and authorities** in Romania or abroad, such as:

- National Bank of Romania (NBR);
- Financial Supervision Authority (ASF);
- National Supervisory Authority for Personal Data Processing (ANSDPCP);
- National Office for the Prevention and Combating of Money Laundering (ONPCSB);
- The Office for the implementation of International sanctions;
- National Agency for Fiscal Administration (ANAF);
- The Competition Council;
- National Archives;
- Courts and other judicial bodies (such as police bodies, prosecutor's offices attached to the courts, National Anticorruption Directorate – DNA, etc.);
- Bank Deposit Guarantee Fund (FGDB), National Credit Guarantee Fund for Small and Medium Enterprises (FNGCIMM);
- Deutsche Boerse Approved Reporting Mechanism (ARM).

e) Certain **Bank clients** with whom you have contractual relationships or other legal relationships related to the banking services provided by us, such as:

- Utility service providers (water, electricity, telephone, Internet, etc.) in the case of direct debit agreements;
- Companies with whom you have employment relationships and with whom we have entered into a salary payment convention agreement.

f) the legal representative of the minor/person deprived of legal capacity or with limited legal capacity.

g) Other partners of the Bank, such as the Credit Bureau (including the transmission of data on payment delays), other financial institutions (for example, correspondent banks and other financial-banking entities participating in payment and interbank communication schemes/systems 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, pension and/or insurance companies, insurance brokers/loss evaluators, Investment Fund management companies providing services for us or, as the case may be, for which we provide various services, other entities (such as banks or financial institutions) in the context of operations related to the assignment or restructuring of the Bank's credit portfolios and/or other rights arising from legal relationships with you.

h) 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) in accordance with the law. To see the full structure of the Group, see: *https://www.brd.ro/despre-brd/noutati-si-presa/ultimele-noutati and https://www.societegenerale.com*

VI. DATA TRANSFER ABROAD

As a rule, we transfer personal data only to states belonging to the European Economic Area (EEA) or to states that have been recognized as having an appropriate level by a decision of the European Commission.

However, we may also transfer your personal data to countries other than the above if:

a) the transfer is carried out **on the basis of appropriate safeguards** (such as, by using Standard Contractual Clauses issued by the European Commission or adopted by the competent authority, together with, where applicable, additional protective measures that we can inform you about, upon request or by using other clauses - subject to their approval by the competent authority, or binding Corporate Rules applicable at BRD level);

b) the transfer is made on the basis of international treaties between the European Union and the third country (for example agreements between the EU and the US);

c) the transfer is **necessary for the performance of the contract** with you, for example if you wish to transfer an amount of money from your account to a bank account located in a third country and thus we must disclose your personal data in order to execute the requested banking operation;

Note: In order to be able to transfer funds abroad, banks (including the Bank) use the settlement services provided by SWIFT. SWIFT temporarily stores data on transactions operated through the SWIFT platform on servers located in the EU as well as in the US. Under applicable law, SWIFT may be required to disclose data stored on US servers to U.S. authorities for anti-money laundering and counter-terrorist financing activities.

d) other cases permitted by law**.**

We may also transfer your personal data to other entities in the SG Group for various purposes under Section **III. Why we process personal data** (mainly point E) and **V. To whom we disclose the personal data.**

VII. WHAT ARE YOUR RIGHTS?

Under the law, you are granted the following rights related to our processing of your personal data:

a) Right of access: you can obtain from us the confirmation that we process your personal data, as well as information on the specific character of the processing, such as: the purpose, the categories of personal data processed, the recipients of the data, the period for which the data is retained, the existence of the right of rectification, erasure, or restriction of processing. This right allows you to obtain, free of charge, a copy of the personal data processed, as well as any additional copies, for a fee;

b) Right to rectification: you can ask us to amend any of your inaccurate personal data or, as the case may be, to complete any incomplete data;

c) Right to erasure: you can request the erasure of your personal data when: (i) these are no longer necessary in relation to the purposes for which they were collected and processed; (ii) you withdrew consent on the personal data processing and we can no longer process them legally; (iii) personal data are processed unlawfully; respectively (iv) personal data must be erased in accordance with the relevant legislation.

d) Withdrawal of consent: you can withdraw your consent on the processing of the personal data processed based on consent at any time, but without affecting in any way the processing prior to withdrawal.

e) The right to object: you can, at any time object to the processing for marketing purposes, including to profiling for this purpose, as well as to processing based on BRD legitimate interest, for reasons pertaining to your specific situation.

f) Restriction: you may request restriction of your personal data processing if: (i) you challenge the accuracy of the personal data, for a period allowing us to check the accuracy of the respective data; (ii) the processing is unlawful, and you oppose the erasure of the personal data, requesting the restriction of its use instead; (iii) the data processing is no longer necessary to us, but you request it for an action before the court; respectively (iv) if you opposed the processing, for the period in which the check is performed on whether BRD's legitimate rights as a controller prevail over your rights as a data subject.

g) Right to data portability: you can ask us, under the law, to supply **the personal data which you provided** in a structured, commonly used and machine-readable format (for example in CSV format). Also, should you request this, we can send your personal data to another entity, if possible from technical point of view. You can exercise your right to portability only if (cumulatively): (i) the processing is carried out by automated means; and (ii) the processing is based on your consent or to perform an agreement with you.

h) The rights related to the automated decisions which we adopt during the course of our business: for details, please see Section IV above.

i) The right to lodge a complaint with the National Supervisory Authority for Personal Data Processing: you have the right to lodge a complaint with the National Supervisory Authority for Personal Data Processing in case you consider that your rights have been breached:

National Supervisory Authority for Personal Data Processing	Blvd. G-ral. Gheorghe Magheru 28-30 Sector 1, Postal Code 010336 Bucharest Romania anspdcp@dataprotection.ro

Note: the right of access, the right to rectification of data, the right to erasure, the right to restriction of processing, the right to object and the right to lodge a complaint with the National Supervisory Authority for personal data processing are also applicable to the agent/representative in the case of clients represented by agents/other forms of representation.

TO EXERCISE THE RIGHTS MENTIONED IN POINTS a) - h) ABOVE, YOU CAN CONTACT US USING THE CONTACT DETAILS PROVIDED IN SECTION VIII (CONTACT).

VIII. CONTACT

Should you have any questions regarding this notification note, or you wish to exercise your rights as data subject, you can contact us using the following contact details: **For the attention of: BRD Data Protection Officer (DPO)**
Mailing address: Blvd. Ion Mihalache, No 1-7, sector 1, BRD Tower, postal code 011171, Bucharest, Romania
E-mail: dataprotection@brd.ro

In the case of clients represented by agents/other forms of representation, the agent/legal representative will inform the Client whom they represent on the existence and content of this Annex "Information on the processing of personal data" and on the fact that this document is available free of charge in BRD units and on the Bank's website, in section https://www.brd.ro/prelucrarea-datelor-cu-caracter-personal.

I, the undersigned, [first name/last name], in my capacity as a client, declare that (i) I have acknowledged and received the document 'Notice Regarding the Processing of Personal Data,' through which I was informed about how my personal data is processed by BRD, as well as about the rights granted to me by law as a data subject; (ii) I have been informed that the document 'Notice Regarding the Processing of Personal Data' is available free of charge on the Bank's website, in the section https://www.brd.ro/prelucrarea-datelor-cu-caracter-personal, as well as at any BRD branch.
Date:
Signature:

I, the undersigned, [first name/last name], in my capacity as Attorney-in-Fact / Legal Representative of the client [first name/last name], declare that (i) I have acknowledged and received the document 'Notice Regarding the Processing of Personal Data,' through which I was informed about how my personal data is processed by BRD in the context of representing the Client, as well as about the rights granted to me by law as a data subject; (ii) I will inform the Client I represent about the existence and content of the document 'Notice Regarding the Processing of Personal Data'; (iii) I have been informed that the document 'Notice Regarding the Processing of Personal Data' is available free of charge on the Bank's website, in the section https://www.brd.ro/prelucrarea-datelor-cu-caracter-personal, as well as at any BRD branch.
Date:
Signature: