BRD
GROUPE SOCIETE GENERALE

BRD-Groupe Société Générale S.A
1-7 Ion Mihalache Boulevard, BRD Tower
011171, Bucharest, Romania
Tel: +4021.301.61.00
Fax: +4021.301.66.36
http://www.brd.ro

SHAREHOLDER EQUITY IN RON: 696.901.518 lei; R.C. J40/608/19.02.1991;
RB – PJR - 40 - 007/18.02.1999; Sole registration no. RO361579; EUID: ROONRC J40/608/1991
Attested by Financial Services Authority (FSA) no. 255/06.08.2008, registered with the Public Register of CNVM under no. PJR01INCR/400008

INFORMATION NOTE ON THE PROCESSING OF PERSONAL DATA[1] FOR LEGAL PERSONS CLIENTS

B.R.D. - Groupe Société Générale S.A., headquartered in Bucharest, 1-7 Ion Mihalache Blvd., 1st District, registered with the Trade Register under no. J/40/608/19.02.1991, Sole Registration no. (UIC/ FIC) RO 361579, registered with the Banks Register under no. RB-PJR-40-007/1999 (hereinafter called "**Bank**" or "**We/Us**"), is processing personal data in its capacity as ***controller***.

Being related to a certain extent to the Client/ future Client, the Bank processes personal data of the following categories of **data subjects** (hereinafter collectively referred to as the "**Data Subjects**", **"You"**): (legal or conventional) representatives of the Client, persons responsible for the management, other persons in key/ major positions within the Client's enterprise; direct and indirect associates or shareholders of the Client; Beneficial Owners of the Client; guarantors and co-debtors, natural persons; members of the above-mentioned persons' families, as appropriate; Authorized Signatories and Delegates; card users; contact persons appointed by the Client; other natural persons mentioned in the documents that the Client made available to the Bank (such as initial owners of the asset to be established as guarantee) or in a relevant relationship with the Client (such as the assigned debtors) or other natural persons whose data is processed by the Bank in order to carry on the relationship with the Client.

I. WHERE DO WE GET THE PERSONAL DATA FROM?

We process the personal data:

- **that the Data Subject provides directly to us**, for instance when the Data Subject acts in relation with the Bank in their capacity as:
  (a) Legal Representative or, as the case may be, Authorized Signatories of a Client
  (b) Authorized Signatoriessign or delegate of a Client
  (c) contact person appointed by the Client or
  (d) guarantors or co-debtor.
- **that we get from the Client**, by their legal or conventional representatives, such as data provided by the Client with regard to the management members, direct or indirect shareholders or associates, Authorized Signatories, Delegates or Beneficial Owners, other natural persons mentioned in the documents that the Client made available to the Bank.
- **that we already have in our database**, for instance when the Data Subject (e.g. the associate or Legal Representative of the Client) is already a Client of the Bank (for instance, as natural person or, as the case may be, as self-employed person).
  Also, we may obtain and process personal data of the Data Subjects from **other sources**, such as:
- **public institutions and authorities** (e.g. ANAF, MFP, ONRC, FNGCIMM, BNR - Central Credit Register (CRC) or Payment Incidents Register (CIP), other guarantee funds, management authorities etc.). For instance, we may interrogate the databases of the public authorities/ institutions in order to obtain certain information, such as: fiscal status of the Data Subjects; including fiscal identification number; should the Data Subject is part of groups of natural persons and/ or legal persons representing a group of Clients
- **electronic registers and databases** (e.g. portal of the courts of law, Credit Register, entities authorised to administer databases with persons accused of terrorism financing and those publicly exposed, National Register for Publicity in Movable Property, ANCP, BPI, OCPI, Official Gazette etc.)
- **business partners**, especially the Bank's services providers. For instance, we may find out new contact details of the Data Subjects (e.g. address, phone number) from the agencies providing claims recovery services to Us, data that the latter ones obtain from their own sources
- **online platforms** (social media and internet) accessible to public, including data aggregators
- **Entities involved in payment transactions** (e.g. international card organizations such as Visa and MasterCard, economic operators accepting card payments, banks and other payment institutions involved in payment schemes). For example, when conducting card transactions, we may receive certain data needed to make payments (e.g., card data, transaction amounts) from merchants who accepted the card payment. Also, in other types of transactions (such as credit transfer, direct debit, debit instruments - check, bill of exchange, promissory note), we may receive your data from a bank/ third-party institution where it was initiated the transaction via interbank payments and communication schemes/ systems (such as SEPA, Regis, SENT or SWIFT)

[1] Drafted according to 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").

- **entities within BRD Group and SG Group**
- **other credit institutions**
- **insurance companies**
- **companies managing pension and investment funds**
- **Central Securities Depository** as company keeping the register of the Bank's shares
- **Other entities**

The Data Subjects' refusal to provide Us certain personal data may cause, under certain circumstances, the impossibility for the Client to have a relationship with the Bank or to contract/ continue to provide the intended product or service.

II. WHICH CATEGORIES OF DATA DO WE PROCESS?

As appropriate, the Bank processes the following categories of data of the Data Subjects:

- **identification data**, such as name, first name, PIN, series and number of the identity card/ another document used for identification purposes (e.g. passport, residence permit, certificate of registration, residence card etc.), as well as other information therein (e.g. date and place of birth, citizenship, gender: masculine/ female, type of ID card, issuing date, expiring date, NIF/TIN codes etc.), signature.
- **contact details**, such as: address of domicile, address of correspondence (business address), e-mailing address, phone number/ s.
- **activity professional data**, such as: information about professional qualification, e.g. information about the profession, the employer's name, the position occupied etc.
- **"know your Clients" information**, e.g. public position held, publicly exposure, special relationships with BRD Group etc.
- **fiscal information** such as country/ countries of fiscal residence and the related tax identification number(s) (TIN)
- **financial data**, such as: information about the economic and financial status, e.g. income, solvency, credit history, equity in commercial/non-profit companies, information about contracts with the same subject matter, entered into with the Bank
- **transaction data such as:** transactional information (such as history of transactions, deposits, saving accounts, opening/maturity date, initial or current amounts/balances, including outstanding amounts, seized amounts etc.)
- **information about fraudulent or, as the case may be, potentially fraudulent activities** both as regards the accepting merchants and of the other Clients, e.g. incriminations and convictions for (attempted) fraud, perpetration of administrative or criminal offences (e.g. for actions of money laundering and/or terrorism financing)
- **data related to the guarantee**, e.g. information about the initial owners of the immovable asset established as guarantee.
- **data regarding the location where certain transactions take place** (e.g. for operations performed at the Bank's **Automatic Machines** or POSs)
- **video recordings** in case the Data Subject visits or transits video monitored areas in one of the Bank's locations/ spaces or makes transactions at the Bank's ATMs. Our surveillance system does not capture by focusing, selective targeting or profiling but only performs continuously or sequentially processed recordings with low or high definition quality.
- video and audio (voice) recordings made during online certification visits, if the Data Subject on behalf of the Client has obtained non-reimbursable funding under programmes implemented by competent authorities, such as: the Ministry of Economy, Entrepreneurship and Tourism, the Ministry of Investment and European Projects, Managing Authorities etc.
- **audio recordings** if the data subject issues on behalf of the Client trading orders that are subject to the provisions of MiFID/MIFIR or submits complaints/ complaints by telephone
- **voice (audio),** 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 "C. Support - Services and complaints managements" below, or on the the occasion of your participation, for the purpose of carrying out the contract with you, in conferences/ video-conferences where recording session has been carried out in and you have consented to the recording of your voice and other data communicated during that conference.
- **any other data necessary or expedient** for carrying-out the Bank's activity, according to law.

III. WHY DO WE PROCESS PERSONAL DATA?

A. ENTERING INTO A RELATIONSHIP WITH THE BANK. PROVIDING FINANCIAL AND BANKING PRODUCTS AND SERVICES. PRODUCTS AND SERVICES MANAGEMENT

We process the Data Subjects' personal data in order to check the Client's/ future Client's eligibility to enter into a relationship with the Bank and to contract the intended banking product/ service.

When responding to a request for contracting a banking product/ service for a Client, we have to verify certain aspects (whether the Data Subject acts as Legal Representative of the Client or whether this one is an affiliate of that Client) in order to make sure that the prudential requirements for entering into contractual relationships with the Client are met.

For the purpose of entering into and performing the contract with the Client, we verify certain aspects in order to prevent and combat frauds and/or to guarantee banking secret.

We are also processing the Data Subjects' data in order to comply with the legal obligations related to the identification of persons accused of criminal offences that may affect the security and integrity of the financial system, the identification of persons accused of terrorism or money laundering actions, etc. The consequences of such verifications may consist in declining the provision of the banking products or services to the Client, in the event that a Data Subject is in such situation.

We may contact the Data Subjects using various channels (e.g. telephone, e-mail, SMS) in order to communicate or obtain different aspects/information related to (i) the status of the contract, (ii) the banking product/ service contracted by the Client or (iii) the exchange rate established by the Bank for payment operations involving foreign exchange transactions from the current day. At the same time, we process personal data for both physically and electronically filing the documents with regard to the Client and the Bank, in order to perform a record service with regard to the documents/ envelopes sent to the Bank during the relationship with the Client, as well as to carry-out some courier activities with regard to the documents/ envelopes containing personal data.

We may process data of the Data Subjects in order to perform the contract entered into with the Client for the record/ courier services with regard to the documents/ envelopes care sent to the Bank during the relationship with the Client.

We may process the Data Subjects' personal data in the context of loans guaranteed by the state or by national or international financial institutions, for the purpose of verifying the fulfillment of eligibility criteria for the approval of the guarantee, as well as for reporting, monitoring, verifying the correct allocation of guaranteed funds and/or the associated benefits. The Bank and the IDB have the capacity of joint controllers, based on the bilateral agreement on the processing of personal data concluded between the two parties, which can be made available to Data Subjects upon request.

In order to carry out the contract with you, we process your data for archiving and storing your correspondence via e-mail and/or other communication platforms (e.g. Teams, Skype, Sourcing Hub).

Grounds:
Compliance with the legal obligations at BRD's charge as well as **BRD's legitimate interest:**
a) to respond to the requests to contract banking products/ services received from Legal Persons, including loans secured with guarantees granted by the state or by national or international financial institutions, and to verify its Clients' eligibility from the perspective of legal regulations and of the prudential requirements for entering into contractual relationships with the future Client, of internal policies and of standards imposed within BRD Group
b) consisting in the need to process the data of the Data Subjects for entering into and performing in an optimal and efficient manner the contracts with the Clients which are Legal Persons in relationships/ legal relations with the data subjects.
c) in order to ensure the general information requirements regarding the monetary conversion fees applicable before the initiation of a payment operation according to the provisions under the national and European legislation in force.

B. ECONOMIC, FINANCIAL AND ADMINISTRATIVE MANAGEMENT. INTERNAL USE ANALYSES AND INQUIRIES

We use the personal data of the Data Subjects for the purpose of organising in an optimal manner and of making more efficient Our activity. To this effect, we may use the personal data of the Data Subjects, *inter alia*:
- to organise some internal databases as support for the activity carried-out by the Bank's structures and divisions
- to improve and optimise the activity of BRD network, as well as Our processes, products and services
- to efficiently organise, carry-out and/ or manage the debt collection and claims recovery activity
- to conduct various financial analyses, in an aggregated format, with regard to the yield of BRD network and its personnel (including the Bank's sales force)
- to draft various reports, in an aggregated format, concerning **(a)** BRD activity and performance on financial and banking markets, as well as **(b)** its exposure towards other financial institutions
- to investigate potential frauds/ suspected frauds in the banking operations
- to support Our position in various inquiries, administrative and legal proceedings, litigations, etc. in which the Bank is involved
- as regards different analyses, internal audit procedures and/ or inquiries conducted by the Bank, on its own initiative or as a result of a notice received from a third party entity (including public authorities)
- to manage the inspections/ inquiries initiated by public authorities.

Grounds:

BRD's legitimate interest in making its activity more efficient and optimising it.

C. SUPPORT SERVICES AND COMPLAINTS MANAGEMENT

We are processing the personal data of the Data Subjects in order to solve their requests or those of other persons, as well as in order to provide you/ them additional information with regard to Our products and services intended for legal entities.

We are making audio recordings of the conversations with the Data Subject in order to improve Our services' quality, as well as in order to prove **(a)** the Client's requests/ complaints with regard to a certain banking product/ service, as well as, possibly, Our answer, respectively **(b)** the Client's consent/ option/ preferences for a certain product or service of the Bank. In case the Data Subject does not wish to have the conversation recorded as above mentioned, this one may contact us, on behalf of the Client, using the available channels, such as by e-mail or by writing us at Our contact address. In this latter case, the actual solution of the Client's request/ complaint will not be affected in any way, but it is possible to have a longer term for solving the same.

Grounds:
Compliance with the legal obligations at BRD's charge and **BRD's legitimate interests (i)** to avoid sustaining any adverse consequences, and **(ii)** to carry-out the activity according to the internal standards and to those established within the group.
The consent of the data subject for having the conversation recorded, as well as BRD's legitimate interest to keep the recording.

D. COMMERCIAL COMMUNICATIONS SENT TO LEGAL PERSONS

Our intention is to keep the Client informed about the news related to the products and services of the Bank and/ or of other companies within BRD group or within Société Générale group that are present in Romania as well as about the products/ services of our partners.

We may use the contact details of the Data Subjects (Legal Representatives and/ or contact persons indicated by the Client) in order to send commercial communications to the Client.

In order to provide banking products and services as pertinent as possible, the Bank analyses the data and information about the Client which may include also data of the Data Subjects. Such analyses do not lead to exclusively automated decision-making.

Data Subjects may object to the processing of their contact details for the transmission of commercial communications sent to the Client, without affecting however the right of the Bank/ of the Bank's partners to send commercial communications to the Client using other communication channels/ other contact details, unless the Client has not withdrawn their consent regarding the reception of commercial communications using remote communication means.

Grounds:
The legitimate interest of BRD and of the Client to receive commercial communications about the products and services of the Bank, of other companies within BRD group and of Our partners (such as insurance companies, pension funds, lease companies).
Consent of the data subject
The contact details of the Data Subjects are processed to this purpose because they are representatives or, as the case may be, contact persons in relation with the Client.

E. COMPLIANCE WITH LEGAL REQUIREMENTS AND INTERNAL RULES

We are processing the personal data of the Data Subjects also in order to comply with the 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 information on public exposure, to ensure that legal provisions relating to Know Your Customer and anti-money laundering are met.
Also, based on the legal obligations that we are bound by, we transmit various reports to pertinent public institutions and authorities, such as: **(i)** reporting of persons subject to FATCA and/ or CRS to ANAF, **(ii)** reports about suspected transactions to National Office for Prevention and Control of Money Laundering Office (ONPCSB), **(iii)** reports about payment incidents to Payment Incidents Register (CIP) within NBP, **(v)** daily reports to ANAF regarding the Central Electronic Register of Bank Accounts and Payment Accounts, **(vi)** reporting based on ANAF requests for information and documents, **(vii)** 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.

Also, we monitor the transactions of Our Clients in order to identify unusual transactions and to prevent frauds. 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 Clients's expected transactional profile based on information provided to the Bank at the time of entering into relationship/ data update for client knowledge purposes. These profiling mechanisms are periodically reviewed to ensure that they remain effective and undistorted.

The processing of data specific to know your client processes also includes the processing of data of third parties such as trustee/ guardian/ guarantor, the information on which is added to the risk score of the client for which it is managed/ guaranteed.

In addition, if the Data Subject has obtained grant funding on behalf of the Client under government programs where the Bank is a partner financial institution, we are required to conduct online, video-recorded certification visits of eligible expenses incurred by the Data Subject from the grant funding.
In view of our membership of the Societe Generale Group, information may be exchanged with entities in the Group, exchanges of information aimed at ensuring compliance with legal provisions relating to client knowledge and the fight against money laundering, thus having public interest considerations.

For some of the processing operations related to this purpose (such as: establishing the data necessary for the anti-money laundering analysis, validating the quality of the data before carrying out the specific anti-money laundering process, creating the model to identify potential atypical transactions to be analysed by Us in order to determine whether they can be considered as suspicious from a money laundering prevention point of view, complying with the regulatory obligations regarding the identification and reporting of suspicious transactions Societe Generale SA acts as an associated controller together with Us. Upon request to either of the two operators, You can receive a copy of the agreement between BRD and Societe Generale regarding the processing of Your personal data. In essence, BRD will only collect and provide Societe Generale with personal data about which it has informed You in advance. To the extent that You submit a request to exercise a right mentioned in Chap. IX Contact below to any of BRD and Societe Generale, they will inform and support each other in order to respond to you within the legal deadline (as a rule, one month). As a good rule, however, Your main point of contact is BRD.
In case of personal data protection incidents that require your prior information, You will be informed by either BRD or Societe Generale.

We can also process your data for the establishment and management of garnishments, the provision of information on garnished amounts to you in BRD's legitimate interest or to enforcement bodies or authorities, in accordance with the Bank's legal obligations.

For the purposes of operational risk management, we may process your personal data in order to comply with our legal obligations to manage operational risk exposure/ mitigate reputational or financial risks, and for the smooth running of processes at the Bank.

Besides the legal obligations, we are bound to observe also some internal requirements / as established within Société Générale Group in relation to drafting the reports and to conducting internal/ external audit which, under certain circumstances, may involve/ have as source personal data processing.

Grounds:
Compliance with the legal obligations specific in this field.
To carry out measures in the public interest, in particular to implement the provisions of Law 129/2019 and Regulation 2/2019, as amended.
Compliance with the legal obligations under MAT Order 1544/2022, GEO 18/2013.

NBR Regulation No 5/2013 on prudential requirements for credit institutions and security measures related to operational and security risks, NBR Regulation No 2/ 2020 on reporting requirements for payment services.

The legitimate interest of BRD and of Société Générale Group so that the Bank carries-out its activity according to the internal standards and to the standards established within the Group.

F. PAYMENT OF DIVIDENDS TO BRD STOCKHOLDERS
Grounds: **legal obligation**

G. 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 and for the prevention of crime.

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.

Proccesing basis:
Legal requirement for situations where legislation requires video surveillance, such as access areas, ATMs, perimeter of cash processing centres, public work area.
Legitimate interest of the Bank to adequately manage the security of the Bank's premises and assets as well as persons.

H. 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.

Proccesing 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 investigations.
Compliance with regulatory requirements to prevent fraud and undue payments.

I. 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.

Proccesing basis:
Legitimate interest of the Bank (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 decision-making, including profiling, which under certain circumstances, may have legal effects on You or, as the case may be, may significantly affect You.

Thus, We make automated individual decisions **by virtue of a legal authorization, including the implementation of public interest measures required in the areas of know your customer, 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 crimes, as the case may be, 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 preventing money laundering and terrorist financing/ implementing International Sanctions. Such mechanisms/ processes can use data collected about You in the know your client process, or data from public sources/ data aggregators, and can even rely on artificial intelligence based models. If, after 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 closed. The use of automated decision-making processes for the purposes of carrying out KYC activity, preventing and combating money laundering and terrorist financing reduces the risk of human error and discrimination, enabling banking services to be provided in accordance with the law, without blocking the enrolment/ transaction management process, and enabling the proper collection and reporting of client and transaction information in accordance with legal requirements.

V. TO WHOM ARE WE DISCLOSING PERSONAL DATA?

We may disclose the personal data of the Data Subjects, as the case may be, to:
a) Our Clients which are related to the Data Subjects.
b) Our Providers of main services, such as:
   - services for interbank payments processing and sending information about interbank operations (e.g. SWIFT - Society for Worldwide Interbank Financial Telecommunication, Transfond S.A. for the national payment systems)
   - services offered by international card organisations (e.g. MasterCard, Visa etc)
   - services offered by providers of payment processing services
   - services for issuing and individualising bank cards
   - services for assessing the assets and other properties

- services for providing terminals used to transfer funds electronically at the point of sale (Electronic Funds Transfer at Point of Sale - POS)
- services for recovering claims and/or collecting debts
- insurance companies
- Custodian of securities
- Chartered accountants
- services of investment agents/ brokers on capital markets or other financial intermediations.

c) Providers of **marketing services**, such as:
- Marketing agencies
- Agencies for market research and surveys
- Agencies for sending marketing communications (e.g. e-mailing commercial offers).

d) Our Providers of **support and/or ancillary services**, such as:
- electronic communications services (e.g. e-mailing, SMS etc.)
- real estate agencies
- bailiffs
- IT services (e.g. maintenance, support, development)
- audit services
- physical and/ or electronic storage and archiving services
- post and courier services
- services for transporting valuables
- legal and notary services or other advice services
- services for the personnel's training.
- electronic signature services on the eSign Anywhere platform provided by Namirial S.R.L., a subsidiary of Namirial S.p.A. (Namirial), as well as the issuance of disposable qualified electronic signatures used for signing documents in relation with the Bank. We submit your identity and contact details to Namirial for the purpose of entering into and executing the agreement for issuance of the electronic signature and signing on the eSign Anywhere platform.

e) **Public institutions and authorities** in Romania or abroad, such as:
- National Bank of Romania (BNR)
- Financial Supervisory Authority (ASF)
- National Office for Prevention and Control of Money Laundering Office (ONPCSB)
- National Tax Administration Agency (ANAF)
- Competition Council
- Courts of law and other judicial entities (such as the police, the Prosecutors' offices attached to the Courts of law, National Anticorruption Directorate - DNA etc.)
- OCPI
- Exim Bank
- Management authorities
- Agencies for Small and Medium Enterprises, Investment Attraction and Export Promotion (AIMMAIPE)
- Bank Deposit Guarantee Fund (FGDB), National Credit Guarantee Fund for Small and Medium Enterprises (FNGCIMM), Rural Credit Guarantee Fund (FGCR), Romanian Counterguarantee Fund (FRC), European Investment Fund (EIF)
- National Property Register (NPR)
- National Supervisory Authority for Personal Data Protection (ANSDPCP)
- Bucharest Stock Exchange (BVB).
  - Ministry of Investments and European Projects (MIPE)
  - Investment and Development Bank (BID)
- Entities with roles in controlling public funds (Court of Accounts, Audit Authority, Ministry of Finance, European Commission, etc.)

f) **Other partners of the Bank**, such as Credit Register, Central Securities Depository, international securities depositories, global/ local custodians, financial instruments issuers, companies managing pension and investment funds, other financial and banking institutions (for instance, corresponding banks, banks of financial institutions involved in syndicated loans and the other financial and banking entities involved in payment plans/ systems and interbank communications such as SWIFT, SEPA, ReGIS, financial and banking institutions to which we confirm or which we request to confirm the signatures and/ or certain information that may be found in the credit worthiness letters, letters of bank guarantee, other letters sent by the Bank's Clients in favour of their business partners, other entities (such as banks or financial and banking institutions) in relation to the operations for assigning or restructuring the portfolio of claims and/ or other rights of the Bank resulted from the legal relationships with the Client etc.), insurance brokers/ damage assessors, external consultants which provide for Us or, as the case may be, for which We provide various services.

g) Entities within **Société Générale Group and BRD Group**, such as Societe Generale Global Solution Centre India (SG GSC INDIA) and Societe Generale Global Solution Centre Romania (SG GSC ROMANIA) under the terms of the law. To check out the complete Group structure, please access: https://www.brd.ro/en/about-brd/profile/societe-generale or www.societegenerale.com.

VI. TRANSFER OF DATA ABROAD

In order to achieve the above mentioned goals, we transfer personal data only to the States within the European Economic Area (EEA) or to the States that were acknowledged to offer an adequate level by a decision of the European Commission. We do not transfer your data to countries outside the EEA.

However, we may also transfer personal data to other States than those mentioned above, should:

a) The transfer takes place **based on appropriate safeguards** (such as, by using Standard Contractual Clauses adopted by the relevant authority, by using other clauses - provided that these ones are approved by the relevant authority, or the Binding Corporate Rules applied within BRD)
b) The transfer is **necessary for the performance of the contract** entered into with the Client, for instance in the event that the Data Subject requests, on behalf of the Client, the transfer of money into an account of a bank located in a third country and thus we have to disclose your personal data in order to perform the requested banking operation.

***Note**: In order to perform a transfer of funds abroad, the banks (including the Bank) are using the SWIFT services for disbursement. SWIFT is temporarily saving the data about the transactions operated through SWIFT platform on the servers located within EU, and not in the United States. According to the laws applicable to SWIFT, this one may be compelled to disclose to American authorities the data they saved on the servers located in SUA for activities related to money laundering prevention and to combat terrorism financing.*

c) Other cases allowed by law.

Data processed by CCTV systems are not transferred abroad.

VII. HOW LONG DO WE KEEP THE DATA SUBJECTS' DATA?

We keep the personal data of the Data Subjects as long as necessary for accomplishing the objectives for which the same was collected, in compliance with the legal provisions applicable in this field, as well as the internal procedures regarding data retention (including the archiving rules applicable within BRD). Once the legal retention deadlines have been completed, the Bank will apply anonymisation of the data thus depriving them of their personal character.

In the 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. By way of exception, in the case of incidents or the defence of any legal interest/right, we keep your personal data 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. WHICH ARE THE RIGHTS OF THE DATA SUBJECT?

According to law, Data Subjects have the following rights related to personal data processing:

a) **Right of access**: Data Subjects may obtain from BRD the confirmation that we are processing their personal data, as well as information about the specific nature of the processing such as: purpose, categories of personal data undergoing processing, recipients of data, period for which the data are stored, existence of the right to rectify, erase or restrict the processing. Such right allows the Data Subjects to obtain freely a copy of the personal data undergoing processing, as well as any additional copies against charge
b) **Right to request the rectification of data**: Data Subjects may request us to modify the inaccurate data of the Data Subjects or, as the case may be, to complete the data that are incomplete
c) **Right to erasure ("right to be forgotten")**: Data Subjects may request the erasure of their personal data when: **(i)** the personal data are no longer necessary in relation to the purposes for which we have collected, and we are processing the same; **(ii)** the consent for the processing of personal data was withdrawn and we are no longer able to process the same on other legal grounds; **(iii)** the personal data are processed unlawfully; respectively **(iv)** the personal data have to be erased for compliance with the pertinent legislation
d) **The right to withdraw consent**: Data Subjects may withdraw at any time their consent for the processing of personal data which are processed based on consent
e) **Right to object:** Data Subjects may object at any time to processing for marketing purpose, as well as to processing based on BRD's legitimate interest, on grounds related to their particular situation. Also, Data Subjects have the right to refuse to receive electronic messages containing information on monetary conversion fees.
f) **The right not to be subject to an individual decision**: Data subjects have the right to request the cancellation or evaluation of any decision based exclusively on processing performed by automatic means, including profiling, which produces legal effects on data subjects or affects similarly to a significant extent.
g) **Restriction**: Data Subjects may request the restriction of processing their personal data where: **(i)** they contest the accuracy of the personal data, for a period enabling us to verify the accuracy of those personal data; **(ii)** the

processing is unlawful, and the Data Subject opposes the erasure of the personal data, requesting the restriction of their use instead; **(iii)** the data are no longer needed for processing, and the Data Subject requests them from us for the exercise of legal claims; respectively **(iv)** in the event that the Data Subject has objected to processing, pending the verification whether BRD's legitimate grounds in its capacity as controller override those of the Data Subject.

h) **Right to portability**: Data Subjects may request, according to law, to receive from us their personal data in a structured, commonly used and machine-readable format. Should the Data Subjects requests us this, we may transmit those data to another entity, where technically feasible.

i) **Right to lodge a complaint with the National Supervisory Authority for Personal Data Processing**: Data Subjects have the right to lodge a complaint with the National Supervisory Authority for Personal Data Processing if they consider that their rights were infringed:

The National Supervisory Authority for Personal Data Processing:
28-30 G-ral. Gheorghe Magheru Blvd.,1st District, Postal Code 010336, Bucharest, Romania
E-mail: anspdcp@dataprotection.ro

FOR EXERCISING THE RIGHTS MENTIONED AT POINTS a) - i) ABOVE, THE DATA SUBJECT MAY CONTACT US USING THE CONTACT DETAILS INDICATED IN SECTION VII (CONTACT). IN THE EVENT THAT THE BANK PROCESSES PERSONAL DATA IN ITS CAPACITY AS A JOINT CONTROLLER, DATA SUBJECTS SHALL HAVE THE RIGHT TO ADDRESS ANY OF THE JOINT CONTROLLERS

IX. CONTACT

For any questions related to this Information Report, or if the Data Subjects intend to exercise their rights, you may contact us at:

BRD: Atten: BRD Data Protection Office (DPO) Address of correspondence:
1-7 Ion Mihalache Blvd., 1st District, BRD Tower, Postal Code 011171,
Bucharest, Romania
E-mail: *dataprotection@brd.ro*
or
Using the dedicated form on the Bank's website at www.brd.ro/contacteaza-ne
or
In any BRD unit by written request (for a complete list of units, please visit page: https://www.brd.ro/en/agencies-and-atms