GROUPE SOCIETE GENERALE

Information Note on the Processing of Personal Data[1]

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, EUID: ROONRC.J1991000608402, (hereinafter called „The Bank" or „Us/ We"), in the capacity of personal data operator, we would like to inform you about the way We process[2] 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, birth certificate, 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, data from the document (birth certificate/court decision) attesting the capacity of legal representative of the minor/ person lacking legal capacity/ with limited legal capacity.
- **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 contractig certain products and services does not imply your physical presence in our units or when your 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?" and on 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.
- **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 regading 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.

[1] 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.

[2] 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).

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 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 clientsClient representatives (e.g. if you are a member of the Clientclient's family), board members of the Bank (if you are an affliliated person), if such data are necessary in the context of legal relations with the Bank'sclientClient.

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.
In order to execute payment transactions initiated by you or in which you are the beneficiary, Transfond SA (Administrator and operator of the Automated Clearing House for Interbank Payments in RON) will have access to the following personal data: IBAN, beneficiary's name and surname, the amount transferred, payment details, 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 to the Payment Scheme administered by Transfond under conditions of legal security and according to strict technical rules.
The complete list of Participants can be found at: https://www.transfond.ro/pdf/Lista%20participanti%20SENT.pdf.

In case of some payment services about which we will specifically inform you prior to their implementation, we may act as associated operators with Transfond SA. One such example is the provision of the RoPay P2P in proximity service, a service for initiating instant payment requests by the payee user, provided to users by the RoPay Scheme Participants (the list of Participants is available at: https://www.transfond.ro/servicii/casa-de-compensare-automata-sent, on the Transfond website), in accordance with the RoPay Scheme set of rules, issued by TRANSFOND SA. BRD is a Participant in the RoPay Scheme. We also act as an associated operator together with Transfond in order to provide the SANB service described in lit. L below.
When acting as joint operators together with Transfond, if you address a request for the exercise of a right mentioned in section VIII. below to either BRD or Transfond, we will inform and support each other so that we can respond to you within the legal deadline (one month, as a rule). As a general rule, your main point of contact is Us (BRD), at the address in section "IX.Contact" below, and if you contact Transfond, it will redirect your request to exercise your rights under the GDPR to Us (BRD).

In the event of personal data protection incidents that require Your prior information, You will be informed, as a general rule, by Us and We will agree in advance with Transfond the content of the information. 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 archiving and storing your correspondence via e-mail.

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 sevices.
- 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 fiancial 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 ans 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 you 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/ curator/ legal representative/ guarantor, information which is added to the risk score of the client for which the aformentioned 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 order to manage managerial supervision and internal control activities on all banking operations carried out at BRD level, we may process your data for the purposes of verifying compliance with legal requirements, identifying and remedying any operational and/or other risks.
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.

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 availabe 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.
In the context of the existence of legal regulations that impose on BRD, as a credit institution, the obligation to ensure a framework for internal control, in accordance with Art. 24 para. (1) of Law no. 129/2019, namely 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 related to payment services.

BRD's legitimate interest and of Société Générale Group to carry out its activity according to internal standars 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.

Proccesing 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.
We process together with Transfond SA, as an operator associated with Us, your personal data (surname, first initial and IBAN code) in order to provide the Beneficiary Name Display Service (SANB) for electronic payments made to accounts opened with a financial institution in Romania that has joined the SANB, with the aim of preventing fraud in the execution of payment transactions and payments not due. The data transferred by Us to Transfond SA is stored by Transfond SA and periodically updated until the termination of Your relationship with BRD and may be queried by other SANB participants in the context described above. The complete list of SANB participants can be found at https://www.transfond.ro/pdf/Lista%20b%C4%83ncilor%20care%20ofer%C4%83%20SANB.pdf.

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 investigation.
Compliance with regulatory requirements to prevent fraud and undue payments.

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.

Proccesing 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);
- Beneficiary Name Display Service (Transfond SA and SANB Scheme Participants).
  The list of participants can be consulted 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, the state institutions and authorities with supervisory and control prerogatives such as: NBR might have access to your personal data.
- RoPay service (Transfond SA and RoPay Participants. The list of participants can be consulted at: https://www.transfond.ro/servicii/casa-de-compensare-automata-sent).
  In the context of payment services administered by Transfond, the state institutions and authorities with supervisory and control prerogatives such as: NBR, might have access to your personal data.
- 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);
- Parteners 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 storage and 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 (ANSDPCP);
- 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) Of the legal representative of the minor/ person lacking legal capacity/ with limited legal capacity.

g) **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 structure, please access: https://www.brd.ro/en/about-brd/news/latest-news and https://www.societegenerale.com

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 if 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 specifc 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 IX (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)
Mailing 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.

The undersigned, _____

BRD Client, I hereby declare (i) having read and received the „Privacy Notice" through which I was informed on the manner BRD processes my personal data, as well on the rights conferred to data subjects; (ii) that I was inforned that „Privacy Notice" is freely available, on BRD website, in section https://www.brd.ro/en/processing-personal-data, as well as in any BRD unit, upon request.

Date _____

Signature _____

The undersigned, _____

As Agent / legal representative of the Client_____ _____, I hereby declare (i) having read and received the „Privacy Notice" through which I was informed on the manner BRD processes my personal data in the context of Client's representation, as well on the rights conferred to data subjects; (ii) that I will inform the Client on the existence and content of the „Privacy Notice" (iii) that I was informed that the „Privacy Notice" is freely available, on BRD website, in the section https://www.brd.ro/en/processing-personal-data, as well as in any BRD unit, upon request.

Date _____

Signature _____