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]
Self-Employed Persons/ Authorized Professionals

B.R.D. - Groupe Société Générale S.A., headquartered in Bucharest, 1-7 Ion Mihalache Blvd., 1st District, registered with the Trade Register under number J/40/608/19.02.1991, Sole Registration no. RO361579, registered with the Banks Register under number RB-PJR-40-007/1999 (hereinafter called **„The Bank"** or **„Us/ We"**), acting as data controller, 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 ("Data Subject", "You").

I. WHAT DATA CATEGORIES DO WE PROCESS?

The Bank processes the following categories of personal data:

- **identification data**, such as name, surname, PIN, ID card serial and number/ other document which can serve as identification (e.g. passport, residence permit, certificate of registration, residence card, etc), 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, NIF/ TIN codes etc.), signature.
- **contact data,** such as: home address/ headquarters, e-mailing address, phone number/s.
- **data necessary for the evaluation of Your eligibility,** such as:
  - information regarding Your professional qualifications, such as information regarding Your occupation, position etc.
  - „know Your customer" information, such as Your public position, publicly 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
  - transactional information (such as transactional history, deposits, savings accounts, 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)
  - any other data, necessary or useful for Bank's activity, as per the law.
- **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 have the right to capture by focusing, selective targeting or profiling, but only performs continuously or sequentially processed recordings in low or high definition quality.
- **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 "D. 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.

II. WHERE DO WE HAVE THE PERSONAL DATA FROM?

We process the personal data that You provide Us, directly, via statement on alternative channels (e.g.: www.brd.ro) or indirectly (e.g. through empowered or other persons representing You in Your relationship with the Bank), or that

[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).

[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).

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, Ministry of PF, ONRC, FNGCIMM, NBR - Central Credit Register or Payment Incidents Register (CIP), other guarantee funds, managing authorities etc.). For example, We can interrogate the authorities/ public institutions databases to obtain certain information, such as: Your fiscal situation; including fiscal identification number; the status of enforcement proceedings You are subject to; Your employee status; information on the status of the claim file by the FNGCIMM; Your identification data in the Central Credit Register, 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. portals of Courts, the Credit Bureau, National Registry of Movable Assets, entities empowered to manage databases with designated persons, subject to international money-laundering sanctions and publicly 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 behavior or other incidents in relation with other banks, **(iii)** if You are included in databases with designated individuals, subject to international sanctions of funds freezing
- **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 card transactions, 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**, particularly 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
- **online platforms** (social media and internet) publicly available, including data aggregators
- **BRD Group entities** (such as data on Customers who had contracts with BRD Finance IFN S.A).
- **other companies for which the Bank provides payment services** (securities issuers, insurance companies, etc.)
- **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 Customers/ Bank's Customers representatives (e.g. if the holder is a member of the Customer's family), board members of the Bank (if the holder is an affliliated person), if such data are necessary in the context of legal relations with the Bank's Customer.

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 customer procedures; We verify if 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).

Grounds:
Entering into and performance of the contract.

BRD's legitimate interest to check its Customers eligibility in terms of internal policies and standards imposed at BRD Group level.
Compliance with legal obligations at BRD's charge.

B. PROVIDING BANKING PRODUCTS AND SERVICES. PRODUCTS AND SERVICES MANAGEMENT

We process personal data to enter into and to perform the contract with You. For fraud prevention and fighting purposes and/ or for preserving banking secrecy: We verify the authenticity of identity documents as well as, where applicable, of other documents that You submit to us; We monitor the way the contract is performed and the associated risks; We apply procedures for conflict of interest management.
We may contact You or, where applicable, other persons (e.g. co-debtors, guarantors) through various channels (e.g. phone, e-mail, SMS, at home), to communicate You/ them various aspects/information concerning the contract, (ii) the contracted banking product/ service or (iii) the exchange rate established by the Bank for payment operations involving foreign exchange transactions from the current day.
For example, if difficulties arise in contract performance, 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 to be cashed, 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 which may include the name and surname of the individual, the amount transferred, payment details, payer's name which may include the name and surname of the individual. 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 the 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 (as a rule, one month). 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 and/or other communication platforms (e.g. Teams, Skype, Sourcing Hub).

Grounds:
Entering into 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. To this end, 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 financial and banking markets, and **(b)** its exposure to other financial institutions
- to support Our position in various investigations, administrative and judicial procedures, litigations etc. in which the Banks is involved
- in the context of various analyses, internal audit procedures and/ or investigations carried out by the Bank, on its own initiative or following the receipt of a complaint from a third party (including public authorities)
- managing controls/ investigations triggered by public authorities.

Grounds:

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 in order 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 prove **(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.
Grounds:
Entering into and performance of the contract, including for processing made upon Your request for entering into 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 Group (insurance companies, pension funds, leasing entities, 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 rely on our internal analyses and studies (for details, please see Section G below).

In line with the aforesaid, We can also send You commercial communications, including direct marketing messages (selling of products and services) regarding the aforesaid partners products and services.
Moreover, 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.

We will send You direct marketing and other business communications only if we have obtained Your consent.

F. MARKET RESEARCH AND SURVEYS

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; to this end, 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 an anonymised format (aggregated data).
If the processed informaion will (also) contain personal data, We will inform You accordingly.
Grounds: **BRD's legitimate interest.**
Your consent - You can withdraw Your consent at any time - for details, please see Section VIII d) below.

G. PERSONALISED OFFERS/ PRODUCTS

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 holder's age, duration of the relationship with the Bank, income/ turnover (including Your previous loan application score), the holder's status of publicly exposed person, the legal person's ownership structure (if is the case), the products and services held and their use on different channels (e.g. internet and/ or mobile banking), analysis of the typology and value of Your transactions over a certain time frame per product (e.g. cards) and/ or per type of retailer
  and/ or
- External sources, such as BRD Group entities or our partners, international card companies, Trade Registry, Credit Bureau, ANAF.

Customizing offers will not exclude Your access to Our products and services.
We analyse and combine dates and informations mentioned above to provide You with the products and services that best fit Your needs and particularities. We may also use the 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 by reference to Your particular situation.
Grounds::
Your consent - You can withdraw Your consent at any time - for details, please see Section VIII d) below.
The algorithms that we apply to customize offers are based on information such as: the duration of service relationship with the Bank, holder's age, income/ turnover (including Your previous loan application), the holder's status as publicly exposed person, the legal person's ownership structure (if is the case), the products and services held and their use on different channels (e.g. internet and/ or mobile banking), analysis of the typology and value of Your transactions over a certain time frame per product (e.g. cards) and/ or per type of retailer. All this information is analyzed to determine a statistical model, which results in the generation of an offer of products and services for You. This offer takes account of Your transactional profile and behavior (as it emerges from the information mentioned above) and will include products and services customized to Your need.
The algorithms used may vary over time, so for more information about the logic used in creating the offers/ products, You may contact us on the information mentioned in the "CONTACT" section.
Sometimes, we use automated individual decisions when customizing offers/ products.
Appropriate guarantees are set in Your favor for the automated decisions we make. So, You have the right to: **(i)** express Your views on that automated decision; **(ii)** to ask us to re-evaluate the decision through a human intervention; respectively **(iii)** to challenge the automated decision.

We will be able to use individual personalized decisions to send You personalized offers if we have obtained Your explicit consent in this regard.

H. ANALYSES AND INTERNAL STUDIES FOR COMMERCIAL COMMUNICATIONS

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: holder's age, based on Your personal identification number) 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

customer profile, to better meet Your needs and expectations. For example, We can include You in a campaign that offers a new product that We are addressing only to customers who have made card transactions with a certain frequency.

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).

Grounds: **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.
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 our legal obligations, We submit various reports to relevant institutions and public authorities, such as: **(i)** reporting of persons subject to FATCA and/ or 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 Register (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)** 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.

We also monitor our Customers' transactions to identify unusual/ suspicious money laundering or terrorist financing transactions, and to prevent fraud. 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 with the Bank/ 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 customer 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 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.

For additional information concerning the reporting made under our legal obligations, You can request this information.

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.

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.

In order to comply with the legal provisions in force, We process personal data through security systems (closed circuit television and visitor's management/ access control) or access record registers, the data being kept for intervals regulated by the law. The data collected under the legislation on the protection of persons, goods and values may be made available exclusively to the authorities, at their request, respecting the conditions provided by the law.

In addition to the legal obligations, We are also committed to complying with a number of internal requirements/ established at the Société Générale Group's level on reporting and internal/ external audit that may, in some cases, involve/ have as a source the processing of personal data.
Grounds:
Compliance with specific legal obligations.
To carry out measures in the public interest, in particular to implement the provisions of Law 129/2019 and Regulation 2/2019, as amended.
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.

BRD's legitimate interest and of Société Générale Group to carry out its activity according to internal standards and those established at the Group level.

J. DIVIDENDS PAYMENT TO BRD SHAREHOLDERS
Processing basis: **Compliance with specific legal obligations.**

K. TO ENSURE THE SECURITY AND PROTECTION OF PERSONS, PREMISES, BANK PROPERTY/ ASSETS AND TO PREVENT AND COMBAT THE VIOLATION OF LEGAL PROVISIONS AND/ OR THE COMMISSION OF CRIMES

We use closed-circuit television ("CCTV") systems to ensure the security and protection of the Bank's premises, assets and persons 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.

***Grounds*:**
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.

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 incorporated in the name of the PFA (which may include the name and surname of the natural person, and the IBAN code) in order to provide the Service of Display Name Beneficiary (SANB) for electronic payments made to accounts opened with a Bank in Romania that has joined the SANB, with the purpose of preventing fraud in the execution of payment transactions and undue payments. The data transferred by Us to Transfond SA are stored by Transfond SA and updated periodically until the termination of Your relationship with BRD and will be available to 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.

Grounds:
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.

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.

Grounds:
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. In this case, the automated decisions will always be based on one of the legal basis provided by Article 22 GDPR, namely **(i)** entering into or performance of a contract; **(ii)** authorization provided by law; or **(iii)** the data subject's explicit consent.

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.

For certain banking products, We use automated individual decision- making 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 credit worthiness, exposure, payment behavior, employer status, debt history etc.

The criteria and the algorithms that We consider relevant may vary over time.
We use automated individual decisions making 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 your online or/ and card payments, 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), 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 E, 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 contest 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
- 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
- services provided by international cards organizations (e.g. MasterCard, Visa etc)
- services provided by payment service providers
- services provided by transaction reporting providers to competent authorities or other regulated entities (e.g. Deutsche Boerse, DTCC)
- cards issuance and personalization services
- debt recovery and/ or debt collection services
- goods and other assets valuation services
- services of capital investment agents/ brokers.

b) **Marketing services providers**, such as:
- Marketing agencies
- Market research and surveys agencies
- Marketing communication agencies (e.g. e-mailing commercial offers); - Partners specialized 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
- staff training services.
- 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.

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)
- 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)
- Rural Credit Guarantee Fund (FGCR)
- Romanian Counterguarantee Fund (FRC)
- European Investment Fund (EIF)
- Managing Authorities
- Deutsche Boerse Approved Reporting Mechanism (ARM).

e) Certain **Customers of the Bank** with whom You have contractual or legal relationships related to the banking products We provide, such as:
- Utility services providers (water, electricity, telephony, internet, etc.), for direct debit conventions
- Companies with whom You have working relationships and have concluded a payroll convention with Us.

f) **Other partners** of the Bank, such as Credit Bureau (including the transmission of payment delays data), other financial-banking institutions (for example, correspondent banks and other financial-banking entities participating in payment schemes/ payment systems and interbank communications such as SEPA, ReGIS, SENT, SWIFT), National Pension House (in the case of pension rights payments through a bank account opened with Us), 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 credit institutions) within the context of assignments or portfolio restructuring

g) Entities from the **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. DATA TRANSFER ABROAD

In order to achieve the above mentioned goals, we may transfer Your personal data only in states belonging to the European Economic Area (EEA) or states that been recognized by a decision of the European Commission as providing an adequate level of protection. Generally We do not transfer Your data to countries outside the EEA.
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 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 necessary for the performance of 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 process 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.

c) Other cases allowed by the law.

Data processed by CCTV systems are not transferred out of the country.

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 Customer, We will keep Your personal data, as a rule, throughout Your contractual relationship with Us, with an additional period of at least 10 years.

Upon request, You can obtain additional information regarding the retention periods applicable to Your personal data.

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. WHAT ARE YOUR RIGHTS?

According to the Law, You have the following rights concerning the personal data processing that We perform:

a) **Right to access Your 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 purpose of the processing, the categories of personal data processed, the data recipients, the period for which the data are kept, the existence of the right to rectification, erasure or restriction of processing. This right allows You to obtain a free copy of the processed personal data, as well as any other extra copies, for a fee

b) **Right to rectification**: You may ask Us to have inaccurate Personal data rectified and incomplete Personal data completed

c) **Right to erasure**: You may ask Us to erase 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 and We can not process them on other legal ground; **(iii)** the personal data are unlawfully processed, respectively **(iv)** the personal data have to be erased for compliance with the relevant legislation

d) **Consent withdrawal**: You may, at any time, withdraw Your consent regarding the processing of Your personal data, data processed on a consent basis

e) **Right to object**: You may object, at any time, to the processing of personal data for marketing purposes, including profiling for the same purpose and You may also object to processing based on Bank's legitimate interest, for reasons related to Your specific situation. Also, Data Subjects have the right to refuse to receive electronic messages containing information on monetary conversion fees.

f) **Right to restriction of processing**: You may request to restrict the processing of Your personal data if: **(i)** You contest 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 refuse the erasure of the personal data and request the restriction of their use instead; **(iii)** the data is no longer necessary for the purposes of processing, but You require them for exercise or defence of legal claims; respectively **(iv)** if You have objected to the processing, pending the verification whether the legitimate grounds of the Bank as data controller override those of the data subject

g) **Right to data portability**: to the extent that we process personal data by automated means and processing has as legal basis the performance of a contract or Your consent, You may ask us to furnish You the personal data **that You have provided us** in a structured, commonly used and machine-readable format (e.g. CSV format). Should You expressly request, We can send Your personal data to another entity, if possible from a technical point of view

h) **The rights attached to automated decisions that We adopt in our activity:** You have the right not to be subject to an automated decision, if it has legal effects on You or affects You in the same way, to a significant extent (see Section G. "Personalized offers/ products" for details). In this case You can challenge the decision, You can request and obtain the intervention of a human operator or You may express Your views on the processing in question

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 infringed.

The National Supervisory Authority for Personal Data Processing	28-30 G-ral. Gheorghe Magheru Blvd,. 1st District, 010336 postal code Bucharest, Romania *anspdcp@dataprotection.ro*

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 data protection notice or if You want to exercise Your rights as a data subject, You may contact Us using the following contact details:

Atten: BRD Data Protection Officer (DPO) Correspondence address:
1-7 Blvd., Ion Mihalache, 1st District, BRD Tower, 011171
postal code, Bucharest, Romania e-mail:
dataprotection@brd.ro