INFORMATION NOTE ON PROCESSING BY BRD OF BRD'S SERVICE PROVIDER REPRESENTATIVE PERSONAL DATA

CONDITIONS FOR THE PROCESSING OF PERSONAL DATA

BY BRD - GROUPE SOCIETE GENERALE SA

BRD - GROUPE SOCIETE GENERALE S.A., registered with Trade Registry Bucharest RO ONRC.J1991000608402, CUI 361579, headquartered in Bucharest, District 1, 1-7 Ion Mihalache Blvd. is committed to dealing responsibly with information we collect and hold about you. In this context we present below the actions we take in relation with your Personal Data, as well as the rights you have as data subject.

I. WHERE DO WE COLLECT YOUR PERSONAL DATA FROM

We collect your Personal Data mainly from you and/your through the supplier you represent, in the context of the contract concluded between BRD and that supplier (hereinafter referred to as **the Contract**). We may also obtain Personal Data about you from the following sources:(i) public databases/online search engines (data on professional and social history), e.g. in case of suspicions regarding the existence of a conflict of interest), (ii) BRD, Société Générale (data on your history, especially if you were an employee/temporary employee provided by them/a person seconded to/by them), other subsidiaries of BRD/Société Générale Group (iii) public authorities/entities or private companies (e.g. incidents, audit, requests for information, (iv) other employees/future employees of the Bank/Group, if they declare that they are related to you, for the purpose of preventing conflicts of interest.

II. INFORMATION WE MAY COLLECT ABOUT YOU

We may collect and process Personal Data about you, such as:

a. **Contact information** - your contact information, telephone number(s), professional email address;
b. **Identification data and official documents** - your identification information, including your national identification number/passport, home address, signature (electronic or handwritten), photo/image (optional);
c. video or static image, your physical presence at the Bank's premises. Our surveillance system does not capture images by focusing, selective orientation or profiling, but only records processed continuously or sequentially with low quality or high definition;
d. business logs containing the technical user assigned to you, your first and last name;
e. the locations where documents containing Personal Data are stored and which are stored on the workstation, in Outlook, SharePoint or shared folders correlated with your first and last name, the name of the workstation;
f. audio or video recordings related to participation in conferences/workshops/training sessions for which the organizers have decided to record the session and you have given your consent for recording.

III. WHAT LEGAL BASIS DO WE HAVE FOR USING YOUR PERSONAL DATA

In the context of processing your Personal Data, as previously mentioned, we act as Data Controller.

We may process your Personal Data for our legitimate interests, such as to exercise and defend a legal right, and our other interests (see details below). When your consent is necessary, a separate consent form may be provided to you, or, as the case may be, the mere communication of data / documents for the acknowledged purpose will be deemed as consent (e.g., you send us health data via e-mail to justify your non-compliance with internal rules).

We may also process your Personal Data that we need to fulfill our legal and/or contractual obligations as Beneficiaries of the services provided by our suppliers. Your refusal to provide us with this information, which are necessary for the performance of the contractual relationship with the supplier you represent, could prevent the execution of the Contract and, implicitly, could make it impossible to provide services or collaborate with BRD.

IV. WHY WE COLLECT YOUR PERSONAL DATA AND JUSTIFICATION OF USES

PURPOSE	JUSTIFICATION
To manage the relationship with the service providers, to conclude, execute and terminate the service contract, to assess the quality of services and training (e.g., in the service assessment process we process data on professional performance and/or general conduct).	Contract performance; Legitimate interest (to enable us to manage our staff efficiently).
Also, as part of our training programs, we may process Personal Data to provide access to our training programs (e.g., through our e-learning platform).	Legitimate interest (to enable us to effectively manage staff); Consent.
To ensure compliance with policies and legal regulations on occupational health and safety, to conduct investigations on occupational accidents and within the control actions of the competent authorities, and to notify you in case of emergency.	Legal obligation (under applicable employment law, occupational health and safety regulations, e.g. those regarding occupational accidents of Service Provider's representative).
In order to grant remote access to BRD's IT systems, for the purpose of providing contractual services.	Legitimate interests (to enable us to ensure the security of the IT systems, of the data and information of BRD and its customers); Contract performance.
For ensuring the security of our IT and electronic communications systems against cyber attacks and IT threats (e.g. computer viruses, intrusions or unauthorized access attempts, denial of service, disclosure of information, internal misuse etc.) for protecting BRD's information, employees' and clients' Personal Data, for fraud prevention and/or detection, operational and reputational risks, we are constantly monitoring the use of computer systems. The monitoring conducted for such purposes complies with the following principles: • it is limited to traffic data, log-in data and data on the use of devices; • content data of electronic communications (e-mail, internet) are accessed only in exceptional cases when legal provisions must be complied with and/or internal investigations must be conducted, if there are reasonable grounds on the perpetration of offenses or breaches of internal policies, instructions, norms and regulations of BRD;	Legitimate interests (to enable us to ensure the security of our systems and premises, as well as personnel); Contract performance; Legal obligation (based on applicable employment legislation, such as provisions relating to information security); Legitimate interests (to enable us to ensure the security of our systems and premises, as well as our staff);

• the content of electronic communications is monitored automatically by the security systems (DLP, sandbox, antivirus, etc.); • where a security incident is identified, we will conduct investigations, and, to this end, we may also use data resulting from the above-mentioned monitoring; • Internet and e-mail connection is provided mainly for fulfilment of the professional obligations by you and, within reasonable limits, it is allowed the use for personal purposes, unless it affects the fulfillment of obligations, systems security or BRD's image.	
In order to verify your compliance with the Code of Ethics of the Bank and/or of the BRD Group, with the internal regulations and legal and prudential rules, we may conduct checks, video and audio monitoring, unannounced inspections, disciplinary investigations, audit missions, during which we may: Identify documents/emails that are not properly archived or are stored for a period longer than the periods stated in the Archival Nomenclature, or access to their content is granted inappropriately. The information collected as a result of these verifications, monitoring, controls and internal investigations may be used in disciplinary or judicial proceedings or provided to the competent authorities, in accordance with legal provisions. Please note that if you store private information on your work devices and/or at your workplace, such as photos, documents or applications, or you conduct correspondence or conversations through professional email accounts, chat, specialized platforms or work terminals, these may be accidentally accessed by personnel authorized to carry out the above-mentioned checks.	Contract performance;
For the purpose of managing operational risks, we may process your Personal Data in order to comply with legal obligations regarding the management of exposure to operational risk/mitigation of reputational or financial risks, as well as for the proper conduct of processes at the Bank.	Legal obligation (e.g. Regulation of the National Bank of Romania (NBR) No. 5/2013 *on prudential requirements for credit institutions* and security measures relating to operational and security risks, NBR Regulation No. 2/2020 on reporting requirements for payment services. Compliance with specific legal obligations in this area, as well as the legitimate interest of BRD and of Société Générale Group in ensuring that the Bank conducts its business in

	accordance with internal standards and those established at group level.
For security purposes and other checks, we store and may access your data regarding authentication in the card access system at the Bank's premises, video images and security codes.	Contract performance; Legal obligation (provisions regarding information security); Legitimate interests (for enabling us to ensure the security of our systems and premises, as well as personnel).
To ensure the security of BRD assets - we may process your personal data in order to protect our assets and verify that you comply with our internal rules. Where necessary (e.g. access paths in BRD premises), video surveillance is carried out to ensure the security and protection of assets, including for preventing and combating crime.	Our legitimate interest in protecting our assets, fighting crime and managing expenses, as well as avoiding being held liable to third parties and identifying inappropriate behavior at the place of activity.
To store and archive emails and communications (via enterprise instant messaging - Skype for business/Teams, or other communication platforms), as well as documents created by you.	Contract performance; Legitimate interest (to ensure compliance with internal storing rules by using a modern solution in the context of facilitating the working methods of BRD employees and providing assistance where necessary to exercise/defend a specific right in court); Your consent in the case of participation in conferences/workshops/training sessions and other similar events where session recording is used.
For internal/external reporting/disclosure purposes – we may process your data for statistics, climate diagnostics, organizational culture and internal reports, as well as for compliance with external reporting/disclosure requirements.	Contract performance; Legitimate interests (to ensure compliance with internal and BRD Group rules and to improve the organization and services we offer, the organizational culture, as well as to comply with certain disclosure obligations); Legal obligation (based on applicable consumer legislation, such as provisions relating to the provision of assistance to customers).
Fulfilling our general legal obligations – such as providing information to government agencies, ensuring compliance with specific health and safety requirements.	Legal obligations; Legitimate interest (to ensure compliance with internal storage rules and to provide assistance where necessary to exercise/defend a particular right in court, as well as for specific legal requirements);
Defending any legal interest/rights/claims in front of official competent bodies.	The legitimate interest in obtaining satisfaction of our interests/rights/rights in court that we have under or in connection with your

	obligations or to defend ourselves in the event that you initiate legal proceedings against us; The legal obligation to retain/disclose certain data for this purpose.
To ensure your safety and protection, as well as to combat violations of legal provisions and/or the commission of crimes. We use closed-circuit television systems ("CCTV") to ensure your safety and to prevent crimes from being committed. Access to video recordings is only permitted in situations that justify such processing, such as security incidents, indications of possible illegal activities by certain individuals, complaints received from other individuals reporting certain prohibited activities captured by video cameras. Launching opinion polls, statistical barometers, climate diagnoses, organizational culture.	Legal obligation for situations where legislation requires video surveillance, such as access areas, public service areas, elevator exits, etc. BRD's legitimate interest in adequately managing your security. The Bank's legitimate interest: based on such surveys, reports/data analyses are obtained regarding the strengths and areas for improvement of the working environment (both operational and regarding organizational culture, behaviors, and well-being aspects).

V. WHO DO WE PASS YOUR PERSONAL DATA TO AND JUSTIFICATION OF USES

RECIPIENT	ROLE
Service Providers of administrative support services for the activity undertaken by us	E.g. security, IT and software service providers, as well as technical support service providers, *back-office*, archiving service providers, accommodation and transportation service providers / tourism agencies, marketing agencies, event organizers, leasing companies, insurance companies, accountants, mail / courier service providers.
Business Partners, clients	Cooperation with these (our partners and clients may be using your data to conclude and execute the contracts entered into by the Bank)
Group member companies (their updated list can be made available upon request)	For the purpose of collaborating with you on assigned projects or for group reporting purposes. For the purpose of storing and archiving e-mail messages and communications (instant messaging enterprise - Skype for business/Teams, trading platforms or other communication platforms) and documents created by you.
Consultancy services providers and any other similar services providers	E.g. lawyers, auditors, accountants, fiscal consultants on various matters of interest for the Bank.

Regulatory authorities, other relevant authorities, public / official databases	Where reporting / registration is mandatory (such as trade registry, authorities, financial reporting, reporting under specific regulations on banking services or financial investment services), etc.
Courts and other judicial bodies (such as police, Prosecutor's Offices, National Anti-Corruption Directorate - DNA, etc.)	In case we receive requests from them according to the legal provisions.

VI. WHEN DO WE SEND YOUR PERSONAL DATA ABROAD?

We may transfer or grant access to your personal data to staff, agents, or contractors in a country outside the European Economic Area (EEA), such as Israel, Switzerland, the US and India, for the purposes and legal bases set out above. We will ensure that any of your data that may be accessed outside the EEA is administered subject to appropriate safeguards. We will ensure that any of your data that may be accessed outside the EEA is managed subject to appropriate safeguards.

Some countries outside the EEA, such as Israel and Switzerland, have been approved by the European Commission as offering protection essentially equivalent to EEA data protection legislation, and therefore no additional legal safeguards are required. In countries that have not received this approval, such as the US or India, we will either ask for your consent to the transfer or transfer the data in accordance with standard contractual terms approved by the European Commission/other approved and accepted safeguards that impose equivalent data protection obligations directly on the recipient, if we are not permitted under applicable data protection legislation to make such transfers without fulfilling such formalities.

Please note that data processed by CCTV systems is not transferred outside the country.

VII. FOR HOW LONG DO WE KEEP YOUR DATA?

We keep records of your data for as long as necessary/to fulfill the purposes for which it was collected and in accordance with applicable legal provisions and internal procedures regarding data retention (including BRD's archiving rules).

Our retention periods are based on legal obligations and business needs, and records that are no longer needed are either irreversibly anonymized (anonymized information may be retained) or destroyed securely, in accordance with the Bank's Archival Nomenclature.

In the case of processing carried out through surveillance cameras, we retain your data for a period of minimum of 20 days, but no more than 30 calendar days.

As an exception, in the event of incidents or the defense of any legal interest/right, we will retain your personal data for as long as necessary to investigate them, i.e., until the completion of legal proceedings in compliance with the applicable legal provisions and internal procedures regarding data retention.

VIII. UPDATING YOUR PERSONAL DATA

We make reasonable efforts to ensure that your Personal Data are accurate. To assist us in this regard, please notify us of any changes to your Personal Data that you have provided to us.

IX. YOUR RIGHTS ON PERSONAL DATA PROCESSING

- **Access**: You have the right to be provided with access to any data held about you by BRD.
- **Rectification**: You can ask us to have inaccurate or incomplete Personal Data amended or supplemented.
- **Erasure** ("right to be forgotten"): You can ask us to erase Personal Data in certain circumstances listed in Article 17 GDPR and we will take reasonable steps to inform other controllers that are processing the data that you have requested the erasure of any links to, copies or replication of it.
- **Withdrawal of consent**: You can withdraw any consents to processing that you have given us and prevent further processing if there is no other ground under which BRD can process your Personal Data.
- **Restriction**: You can require particular Personal Data to be marked as restricted whilst complaints are resolved, and also restrict processing in certain other circumstances. If, following your request, we restrict the processing of your personal information, BRD will store your personal information, and otherwise process it, only with your consent; to establish, exercise, or defend a legal claim; to protect the rights of another natural or legal person; or for reasons of important public interest. We will also inform you before lifting the restriction of processing;
- **Opposition**: You have the right to object to processing of your Personal Data when this processing is grounded on BRD's legitimate business interests. We will stop processing such data information unless: (i) there are compelling legitimate grounds for the processing that override your interests, rights and freedoms; or (ii) BRD needs to continue processing your personal information to establish, exercise or defend a legal claim;
- **Portability**: You can ask us to transmit the Personal Data that we hold about you to you or to a third party, electronically (i.e. in a structured, commonly used and machine-readable format), whenever we process your data based on contract/consent and via automatic means.
- **Raise a complaint to the Supervisory Authority**: You can file a complaint about the way we process Personal Data with the data protection authority:

National Authority for Supervision of Personal Data Processing (ANSPDCP)
B-dul G-ral. Gheorghe Magheru 28-30, Sector 1, postal code 010336, Bucharest, Romania
www.dataprotection.ro

X. YOUR CONTACT FOR ANY QUERIES

BRD has designated a Data Protection Officer whom you can contact if you have any questions regarding the implementation of the Internal Data Protection Policy or this Information Note (including safeguards we apply in relation to the export of your Personal Data) and/or you wish to exercise your rights in relation to the processing of personal data provided at chapter VIII.

The contact details are set out below:

- Attn: BRD Data Protection Officer
- Address: BRD GSG- TURN BRD, 1-7 Ion-Mihalache Blvd., District 1, Bucharest
- Phone: 021.301.4381
- Email: pdpo@brd.ro.

Notification of the conditions for the processing of Personal Data

The Bank will inform through the electronic correspondence whenever changes occur that may modify and / or supplement the Conditions for the processing of Personal Data, such as, changes regarding the categories of data processed, the purposes for which they are processed, the conditions of transfer of the data abroad and / or any other modifications thereof.

By signing this Information Note, I declare that I have read and understood the provisions of this document which contains information on the manner in which my Personal Data are processed by the Bank, as well as on the rights I enjoy under the legislation in force.

At the same time, I declare that I have become aware, as representative of the Service Provider [...], of the existence of Contract No. [...] dated [...] concluded between this Service Provider and BRD, as beneficiary of the services.

This document has been drawn up in two copies, each with equal legal force, one for the Bank and one for the Representative.

Name and Surname:

Date:

Signature: