User Charter for Information Protection and Use of IT Resources

Considering:

1. The contract concluded between the **Service Provider** and **BRD-Groupe Société Générale** (hereinafter "**BRD**"), (hereinafter referred to as "**the Contract**");

2. The specific of the activity performed by BRD, which, as a joint stock bank company, has the obligation to maintain confidentiality on the facts, data and information at its disposal, in accordance with the specific legislation of the financial-banking field, through capital market specific legislation as well as with the specific legislation for the processing of Personal Data;

3. The fact that the Service Provider, its representatives, employees and collaborators involved in performing the Contract, have access and use, mainly, data of a confidential nature (hereinafter referred to as Confidential Information – see Glossary).
4. The protection of BRD's Information Assets and Information System is a key stake. This protection is everyone's responsibility.

The following charter confirms BRD's desire to:
- Protect its Information Asset and its brand image.
- Ensure a fair and responsible use of its Information System.

The Service Providers employee/collaborator/subcontractor (hereinafter referred to as "the User"), acknowledges the provisions of this Charter.

Objectives and scope
Objectives
BRD provides to all Users of its Information System a set of IT Resources as well as information and data needed to accomplish their missions. The use of these resources requires each User to comply with the rules laid down by BRD and the controls carried out to enable BRD to protect itself against all types of risks such as fraud, information leakage, unavailability of its Information System, cybercrime and regulator non-compliance.

This Charter sets the rules to ensure the security and performance of the Information System, to preserve the data confidentiality in compliance with the laws in force and the rights and freedoms recognized to Users. The examples mentioned in this charter are not exhaustive.

The Charter shall be annexed to the Internal policies and shall have the same effect as such.

Due to the continuous evolution of technologies, this Charter may be subject to changes.

Scope of Application
Each User of the Information System or who may hold BRD Information Assets must comply with it.

Charter communication mode
This Charter is binding to each User of the Information System or Information Assets by signing it individually.

The Charter is communicated to the Service Provider, if necessary, at the signing date of the Contract. The Service Provider communicates this Charter, prior to the start of the activity and the granting of access, to all its employees, collaborators, representatives who, exceptionally, are to be granted access by BRD to the IT System or to BRD's Information Resources. Subsequently, the Service Provider sends to BRD the Charter signed by each User, by email, to the email address of the BRD's contract manager.

- For Users that use a direct method of connecting to the BRD Information Systems:
  The User declares that he/she has been informed and expressly acknowledges that the provisions of the Charter, BRD regulations and procedures mentioned in the Charter are continuously available in the BRD's information system at the link https://intralegis.apps.brd.ro/intranet/ to which he/she has unrestricted access at any time, and cannot invoke the non-receipt of any regular information or amended versions thereof, assuming the obligation to consult them periodically and to keep himself/herself informed of their content.
- For Users that use a dedicated VPN solution to connect to the BRD Information Systems:
  BRD undertakes to inform the User, directly or through the Service Provider, about the rules contained in the Charter, in case of significant changes, and the User undertakes to aknowledge their content and to send the signed Charter to BRD, to the e-mail address of the BRD contract manager, directly or through the Service Provider, within 5 days of their communication by BRD.

Rules for information protection and use of IT Resources
Respect of Information confidentiality
Information Classification
When using BRD's Information System, the User must apply the general principles:

Confidentiality of the information held on all aspects related to the activity carried out in BRD, regarding its clients, as well as any other Confidential Information of which it becomes aware in the course of its activity, in accordance with BRD 's privacy policy.

- Respect of bank secrecy.
- Personal Data Protection.
- Inside Information Protection.

To do this, the User commits to defining and updating the Confidentiality level of the information contained in the documents / messages (not structured data) that they are required to create or modify according to the four-level scale: C0-Public; C1-Restricted; C2-Confidential; C3-Secret and to respect the associated rules of use. For C2 and C3 there is a sublabel "Can Leave the Group/Cannot Leave the Group".
Privacy classification is also performed for structured data (databases), which can be accessed through IT applications provided by BRD.

Data protection
The User commits to protecting the Group's Information Assets, in particular by respecting the following rules:

- On BRD's premises, clean your desk and secure your documents and equipment before leaving them unattended (computer lock, session log off, anti-theft cable, locker, etc.).
- Ensure that confidential information is not left in meeting rooms.
- Limit printing and use devices according to the Confidentiality level (garbage can, secure container, shredder, etc.) for their destruction.
- Outside BRD's premises, make sure to use all means of theft prevention (anti-theft cable, hotel safes) and protection of disposed information (computer lock, session log off, privacy filters, etc.), in order to reduce the likelihood of theft of equipment or information.
- Remain vigilant regarding the risk of information disclosure in crowded places (public transportation, elevators, restaurants, etc.) by adopting the strictest discretion regarding one's professional activities.
- Do not participate in telephone meetings in public places.
- Strictly limit confidential paper documents and their circulation outside BRD's premises.
- At home (home working or on-call duty) or in another remote location (example of working from one's premises for a service provider), ensure that confidential or non-public information is not

seen, heard or shared with unauthorized third parties who may be present, remain vigilant about the presence of any connected objects (security camera, voice assistants permanently connected etc.), in case of absence, close the work session and protect paper documents from prying eyes.

- Remain vigilant about any unusual request from an unsafe source (phishing, fake president fraud, etc.) and contact your security correspondents in case of doubt, for example to call back on a telephone number the person who called.
- Respect the visitor accompanying process in effect in BRD's premises.

Personal Data Protection

The General Data Protection Regulation (GPDR) and the Bank's norms (N1D81, N1D81I1) define the conditions under which the processing of Personal Data may be carried out and the rights of the persons concerned by the processing. Thus, the User, in the context of their professional activity and the execution of their missions, must act in accordance with these policies and respect the fundamental rights and freedoms as well as the privacy of individuals. More specifically, the User must ensure that the processing of Personal Data that they may be required to carry out in the context of their professional activity, comply with the data protection policies applicable to their perimeter and the internal policy for the protection of Personal Data.

The User acknowledges that Personal Data processed of behalf of BRD shall not be communicated or used in any form whatsoever for purposes that are foreign to or contrary to the mission entrusted to them under the contract, for personal purposes or in the context of activities outside the Bank.

In case of questions regarding the regulations related to Personal Data Protection, the User is invited to contact the Data Protection Unit (PDPO) by mail pdpo@brd.ro

Assuming that the User is at the root cause of a Personal Data breach (loss of availability, integrity or confidentiality of Personal Data), he/she must notify as soon as possible the persons referred to in the procedures in effect within BRD (N1D81I1P1) for the relevant departments to inform, if necessary, the supervisory authorities concerned within 72 hours from the date of becoming aware of the incident concerning personal data and, if applicable, inform the persons concerned by the presumed data breach.

General rules for using the BRD's Information System

User Responsibility

Access to BRD's IT Resources is provided to Users for professional purposes and according to business needs. This means that a message sent or received from an IT resource provided to the User is of a professional nature unless used in the context of paragraph 2.2.3 "Private use".

Each User is obliged to inform himself/herself regularly of the applicable rules of the use of the Information System and the protection of BRD's information, by directly accesing them at the linkhttps://intralegis.apps.brd.ro/intranet/

Each User is thus responsible for the use they make of the IT Resources provided to them.

In the event of the deterioration of the equipment and in the absence of any negligence or fault on the part of the User, BRD will bear the cost of the equipment.

The Responsibility of the User will be engaged if they are personally accountable of a non-compliant use. In this regard, authentication and Traces are means to reveal the User's identity.

Failure to respect the defined rules in this Charter may result in the application of disciplinary measures for its author, in an appropriate and proportionate manner, in accordance with the scale of the sanctions provided in the internal rules of procedure. Example of failure to comply with the applicable rules can be considered as a misconduct/ conduct incident:

a. For all Users: sensitive (C2 or C3) information leakage, storing clear text password, repeated consultation of suspicious attachments or links, downloading and installing un-approved packages or bypassing security rules.
b. For the ICT professional population, the rules specific to their function also apply, and may therefore be considered as a breach of these rules storing & sharing admin/service passwords or secrets,

using password on admin/service account not compliance with internal rules, bypassing security process or not implementing security by design.

The User must contact their Security Correspondent (CyberAlert@brd.ro) or their hierarchical superior as soon as they suspect a security breach or a potential attack on the BRD Information System. They are not responsible of alerting the other Users.

Access to BRD/Société Générale's resources

Each User receives individual access rights to the Group's Information Systems through confidential authentication means (confidential codes, smart cards, etc.). This access right cannot, in any way, be transmitted, even temporarily, to a third party without engaging the responsibility of the User. The means of authentication are strictly personal and must only be used for the User's own use. The User is responsible for their confidentiality.

Therefore, the User must in particular:

- Choose confidential codes that comply with BRD's password policy, including complexity requirements, keep them secret and update them according to the frequency set by BRD or as soon as it is suspected to have been compromised (Attention! Remote change of the domain access password - Windows password - is only possible during its validity period)
- commit not to give to unauthorized Users access to information systems, through materials they use,
- Lock its software / system session before leaving Equipment unattended,
- Not use or attempt to use any User account other than one's own or hide one's true identity,
- Not bypass/deactivate the means of security and monitoring (e.g screen-saver, settings, prevention tools for malware, EDR, DLP, AIP).
- Not use their access right to the Information System for purposes other than those for which the access right has been granted.
- Not to leave unattended the smartcard - which he/she must have with him/her at all times - and/or the phone where the Mobile Phone Soft Token application is installed; never to communicate to anyone the PIN of the phone and the PIN of the OTP application.
- Not to connect to the data network of the BRD premises any devices other than those authorized.
- Use the resources of the Information System within the strict framework of its professional activity, defined by its function and within the limits of their attributions or the delegations granted to them. Information classified above C0-PUBLIC level may only be used or consulted exclusively for business purposes and under no circumstances should it be used or consulted for personal reasons or to satisfy one's curiosity.

1.1.1.1 Remote Access to BRD Information System

For remote access to the BRD Information System, a VPN solution is used. If using the VPN TMA solution provided by BRD, the user additionally receives an access account in the SG Group solution.

1.1.1.2 Rules for remote access to BRD Information System

i. Do not use public Internet access points (eg free WiFi, airport, restaurants, hotels, etc);
ii. Legitimately use your own internet access point with superior security features (eg minimum WPA2 WiFi router - with complex password, hotspot on the Service Provider/BRD mobile phone, set with complex password). Do not share your WiFi equipment with others nearby;
iii. Do not use the video recorder or screen recorder to extract information from the work device;

The User's access right automatically ceases when they leave the Service Provider/BRD (exit from the workforce, resignation or end of contract). It can also be modified during a change of assignment and/or according to business requirements.
The User may be granted Privileged Access Rights to the Information System that they can only exercise for the purpose for which these rights were granted to them. In case the User has privileged access rights, the User must comply with the specific rules in section §2.4. Obligations related to the use of privileged access accounts.

Private Use/Personal use

Reasonable private use of the Information System (accessing websites, sending e-mails, file storage, telephony, printing, photocopying, scanning, etc.) is tolerated within the daily needs and family life framework. This tolerance is subject to the respect by the User of the principles set out in this charter.
The private use must be limited, both in duration and frequency and must not have an impact on the User's professional activity.
In the context of a private use of the information systems, the User is required to:

- If they use a file directory, to identify the name of this directory by the keyword "[prv]" or any other clear and unambiguous identifier of the private nature of the information.
- If printing a private document, identify the name of the document by the keyword "[prv]".
- If they issue e-mails or any other form of message (e.g. sms), mention in the subject field the keyword "[prv]" (or at the beginning of the message when the subject field does not exist).
- If they wish to receive e-mails or any other form of messages (e.g. sms), to have the sender mention in the subject line the keyword "[prv]",1 (or at the beginning of the message when the subject field does not exist). Each User must inform their correspondents when communicating their e-mail address on a private basis. These messages will be subject to the same technical inspection procedures as those defined in §3 "Control measures and supervision".

No information of a professional nature can benefit from the keyword [prv]. As such, it can neither be stored in the file directory "[prv]", nor be printed, photocopied, scanned with the keyword "[prv]", nor be issued or received by the User in e-mails or in any other form of message with the subject "[prv]". BRD reserves the right to block the output of a message or document marked "[prv]" if professional information is detected (see §3 "Control measures and supervision"). Users will then receive an email informing them of the automatic blocking of this sending and may refer to their hierarchy for any request to unblock the sending of said message.

The private use of the Information Systems is the sole and entire responsibility of the User. BRD will not put specific security measures for the protection of private content.
If it turns out that precise and consistent indications prove that the User is engaged in a malicious or abusive use of the keyword "[prv]" or the possibility left to their to use the company's resources for private purposes, BRD will be entitled to draw all the disciplinary and possibly judicial consequences.
The misuse of the "[prv]" tag may be deducted also from the content automated detection, the frequency of messages received or sent, the volume of data exchanged, stored or printed, the attachments and connection duration.
BRD will be able to read the content of messages and private files based on the respect of the regulations in force, and particularly the secrecy of correspondence.

Rules for using professional digital equipment and tools

The tools and User accounts used in the professional context must be those authorized by BRD.
Non-exhaustive list of examples:

File exchanges must be carried out through tools validated by BRD in compliance with confidentiality rules. For example, the use of cloud platforms for transferring large files (e.g. WeTransfer) is

[1] Regardless of accents or lowercase/uppercase; will therefore be accepted for example "

[Prv], [pRV], ... »

discouraged, and the use of SG Group solutions is favored. For transferring documents between 5MB and 2GB in size internally/from external BRD, the tools provided by the BRD should be used: Secure Share. For external BRD transmission, it is necessary to obtain authorization from the CISO. For larger volume transfers, the use of the SecureHub solution is recommended.

The use of external storage media (mobile hard disks, USB sticks, memory cards, CD/DVD, optical writers) is also a major risk factor and is implicitly prohibited (details in N10D1I5).

Any exchange of messages on sensitive, strategic or commercial subjects must be carried out through tools validated by BRD/Société Générale, including tools like mobile devices like smartphone.

All professional identifiers must be used in a strictly professional context and must not be communicated on websites not authorized by BRD.

A personal (i.e. non-professional) e-mail address must be used to register on external sites (excluding authorized professional activities).

Automatic transfer of business email to personal (i.e. non-business) email is not allowed. The transfer to the professional email of another employee, or to a professional shared email can only be done at the initiative of the employee itself. When the professional context requires it, and if the transfer of the email is not implemented, the employee will have to set their e-mail to send a message designating the person(s) to contact during their absence.

Due to the risks associated with sending internal BRD documents to private e-mail addresses, this is implicitly prohibited.

Rules for using Equipment

Whether for Equipment provided by BRD or for Personal Equipment used for professional purposes (BYOD), the User commits to taking the necessary measures to guarantee the security of professional information and must in particular comply with the following rules:

- Remain vigilant about Equipment Access by third parties.
- Respect the basic configuration of the Equipment or the standard BRD or the secure solution deployed on the Equipment.
- Perform the required maintenance and updates.
- Notify user support (MyIT_Support@brd.ro)and/or its Security Correspondent (CyberAlert@brd.ro) in case of a failure, malfunction, alteration, theft, loss or security breach of the terminal (laptop or smartphone).

In addition, with regard to Personal Equipment used for professional purposes, the User also undertakes to comply with the rules concerning the access right described in paragraph 2.1.1 "Information Classification " as well as the confidentiality rules referred to in paragraph 2.1.2 "Data protection".

By using your own equipment for professional purposes, you also accept the associated security rules, respectively:

i. the installation of protection applications against cyber threats (eg antivirus, VPN tunnel, application firewall, containerization, etc.), up-to-date;
ii. the operating system to have the security patches applied up to date and patches on all software components used (browser, software applications, etc.
iii. compliance with the rules in §2.2.2 Access to resources

Certain public, non-mastered or non-approved applications by Société Générale, may nevertheless be accessible to the User. These applications present risks and may in particular collect information without the User's knowledge such as technical data (device type, OS version, etc.), usage data (date and time of

installation, use, etc.), but also certain personal data elements (geolocation, age, preferences, etc.). The use or download of these applications for professional purposes from the Equipment can only be done after having been previously validated by the security teams. They can be requested at MyIT_Support@brd.ro (if the equipment belongs to BRD), they are only installed by the IT support technician after they have gone through the approval circuit.

Rules for using the Internet

1.1.1.3 Internet browsing

BRD provides Internet access to all Users of its Information System according to its business needs. Only websites with a direct and necessary link to the professional activity carried out are intended to be consulted. BRD reserves the right to filter site categories by default and block downloads on certain sites. The associated rules and processes are governed by the Internet Browsing Filtering Policy.
The User must be particularly vigilant with regard to the content consulted, downloaded and exchanged on the sites with the Internet access provided by BRD. In particular, it is forbidden to:

- Transmit or publish confidential or non-public–Information about BRD, its subsidiaries or more generally about BRD entities, its customers or partners, or its workforce (unless authorized by the hierarchy and protected by adequate validated means).
- Download, transmit or store content of a pornographic, pedophile, racist, xenophobic or violent or defamatory nature, containing any incitement to hatred, undermining respect for the human person and dignity, inciting the commission of any offence or crime, glorifying terrorism, or any content that is contrary to public order or offensive, or that infringes on Société Générale's internal or external brand image.
- Commit reprehensible acts with regard to applicable law, in particular with regard to respect for intellectual property rights.
- Participate in gambling.
- Carry out a commercial activity in a private capacity.
- Create or administer Internet or electronic communication services unrelated to the needs of their professional activity.
- Access to external e-mail services (webmails), external instant messaging (chat) and social networks. Access to certain social networks is granted on a waiver basis for business use.

The downloading of programs is only allowed to persons explicitly authorized. The User must take care not to overload the Société Générale Information System in an abusive manner, in particular by limiting transfers of large files or access to certain multimedia resources.

1.1.1.4 Social networks

As part of professional use of social networks, the User shall refrain from disclosing confidential information about BRD, their professional activity, the roles and responsibilities of their colleagues or their clients and undertakes to follow the communication rules issued by BRD, particularly with regard to respect for banking secrecy. The User must not engage in controversies that pose a risk to the image of BRD.
Furthermore, messages that are offensive, denigrating or likely to infringe on the privacy, image or reputation of employees and the company are prohibited. BRD will be entitled to draw all disciplinary and possibly judicial consequences.

Rules for using messaging and internal communication tools

BRD provides Users of its Information System with a set of means of communication (e-mail, instant messaging, internal communities, etc.).
It is forbidden to transmit, retransmit or publish messages of a defamatory, abusive, denigrating or likely to infringe the privacy of persons, the image, reputation or consideration of persons and messages that would be contrary to the laws in force. Such messages could engage the responsibility of the User and Société Générale.
The User must not transmit messages such as false alarms or rumors (unverified information likely to mislead someone).

The User must strive to limit the number and size of attachments to avoid overloading the network. they must also use mailing lists with wisely and avoid sending copies to an unjustified number of recipients.
To receive/send sensitive information internally to BRD/SG Group, secure your messaging using an internal digital certificate. The internal digital certificate allows the use of the "Encrypt" function to protect the content of the message and/or its attachments sent only internally to BRD/SG Group. The transmission of sensitive information externally BRD/Group SG is done by archiving and password according to the Guide for password sensitive documents, using complex passwords.
If the User receives a suspicious message (unknown user or unusual message from a known user or any other suspicious message), he/she should press the "Suspicious Message" button.

Obligations related to privileged access

For each person having a privileged account on a workstation/server (physical or virtual). An account for privileged access on the workstation/server has been provided to you as a part of your activities. Holding an account for privileged access is a high responsibility to protect information security.

Rules:

- *Use a dedicated, quasi-nominal, account for admin actions;*
- *When you are defining a password, ensure that the password comply with Société Générale and/or BRD password policy (Ghid 50). The password must be changed on a regular basis;*
- *Only install applications from a trusted origin (editor website must be preferred), with no malicious or illegal purposes;*
- *Ensure that the application you want to install is not already available in the Service Catalog. Additionally, ensure to comply with license issues;*
- *Keep the application up-to-date, and perform the update as soon as the editor make the update available;*
- *Only ask for a privileged account when this usage is strictly needed, and not systematically;*
- *Do not give your admin credentials to anyone;*
- *Do not stock your password in plain text on a physical (e.g. post-It) or logical (e.g. text file) support.*

The following actions are prohibited:

- *Create or move a user to the Administrator Group;*
- *Edit the other Groups;*
- *Edit System privileges or Groups used by services;*
- *Edit or remove security parameters of the workstation/server;*
- *Edit or alter the features of security tools;*
- *Edit the configuration of the workstation/server for any purpose without the express written permission of CESI (derogations process – according to **Appendices 4-12** of **N10D1I5**);*
- *Install a program (tool, software, freeware,etc.) without the express written permission of your manager and CESI (derogations process – according to **Appendices 4-12** of **N10D1I5**).*

Each person who has a privileged access account to work on the workstation/server (physical or virtual), shall respect the rules listed above. Sign this charter is not justification for requesting the local administrator right. It certifies that you are aware of your obligations for the usage of this type of account.
Moreover, each person concerned by this document must act under the legislation, the national law, rules, procedures within BRD and good practices related to his activity. Non-compliance of the above can have legal consequences.

Control measures and supervision

BRD reserves the right to monitor the use made of IT Resources and Information Assets, in compliance with the legal framework and the privacy of Users to:

- Ensure the security of the Information System and the Information Asset.
- Ensure compliance with the rules defined in this charter.
- Fulfil the obligations arising from the laws and regulations governing the activities of credit institutions and investment firms.

Control Measures and Traces

Control measures can thus be put in place in order, for example:

Check the installed software on the workstations provided by BRD, in order to ensure that no malicious software compromises the User's computer.

Verify that the protection mechanisms put in place by BRD on professional and personal Equipment used in the professional context are not deactivated.

Control the content of e-mails or any other form of messages / files / directories / documents that are stored / sent / transferred / printed in the software and equipment provided by BRD in order to ensure the security of the Information System and Information Assets.

Block e-mails that contain documents identified as not being allowed to leave the BRD. Users will then receive an email informing them of the automatic blocking of this sending and may refer to their hierarchy for any request to unblock the sending of this email.

Filter the flows exchanged on the Internet.

Block access to unauthorized sites.

More generally, any control measure necessary to preserve the security of BRD's Information System and Information Assets may be implemented.

The functioning of the control measures is the responsibility of the system administrators whose duty of confidentiality is set out in paragraph 3.3 "Duty of confidentiality of system administrators" of this charter.

In compliance with the principles of transparency and proportionality, Users' attention is drawn to the fact that the computer security devices (firewalls, access control systems, etc.) set up by BRD generate Traces of systems that make it possible to identify events (authentication to a session, deletion of files, use of applications, etc.). These Traces can then be correlated amongst one another to investigate the causes of an event that has or could potentially impact the security of Information Assets and Information Systems.

The Traces collected by BRD include the following information (non-exhaustive list):

Sent or received messages:

- All the resources accessed by the User through Internet with details such as the technical connection parameters (including the User account ID, date and time, volume of data transmitted...).
- User authentications access to IT Resources with details such as the date and time of access.
- List of technical parameters necessary for the management of e-mail services (User account identification, recipient's contact details, date and time, volume, format and nature of attachments, etc.).

Traces may be retained in accordance with the relevant internal policies and applicable regulations.

Exploitation of the Traces
For operational purposes, a statistical exploitation of the Traces is carried out, in anonymous way. It consists, in particular, of establishing statistics on the connections and contacts made.

Nevertheless, BRD may carry out nominative audits on the Enterprise Traces, following a malfunction, a security alert or the presumption of non-compliant use of IT Resources, while respecting the secrecy of private correspondence referred to in paragraph 3.3 "Duty of confidentiality of system administrators".

In this case, the material findings are intended to identify the various circumstances that will enlighten BRD/Société Générale on the possible realization of a non-compliant use and on the identity of its author.

System Administrators' Duty of Confidentiality
System administrators ensure the normal operation and networks and systems security.

Consequently, by their very functions, they can have access to all the information related to Users.

They are bound by a duty of confidentiality and must respect the processes and rules related to their activity.

In this context, the Administrators must not disclose these information when it is covered by the secrecy of private correspondence or falls within the privacy of Users and does not question the proper application technical operation, nor the security, nor the interest of the company.

Technical and administrative measures
For technical or administrative purpose, access to IT resources may be suspended, restricted or deleted, individually or collectively, when necessary, in particular in order to maintain the availability or integrity of BRD's Information System and the protection of BRD's Information Assets.

Normative Documents
N1D41I2 – „Information Classification and Protection"
Guide 50 – „Identification and authentication of users in BRD information systems"
N10D1I5 – „Information Security Rules Applicabile to Access Devices (fixed and mobile) to BRD IS, Electronic Communications and Collaborative Work and External Storage Devices. Derogation Management
N1D81 – Protection of Personal Data
N1D81I1 - Processing, Protection and Security of Personal Data
N1D81I1P1 - Personal Data Security Breach Management

Glossary
Confidential Information: all information which may only be communicated to Users on a need-to-know basis, and the disclosure of which would have a high-level impact for BRD or for the Group, its entities or the person or people concerned. Inside information is included at least in this level of classification. Examples of Confidential Information:

a) Information regarding the activity performed by the BRD – in this category is included, without being limited to, the following: information/data regarding platforms and configurations of informatics system, know-how, creation or experimental work, ideas, concepts, techniques, specifications, drawings, sketches, charts, software, encodings, source code, operations related to installation, use and/or maintenance of software/hardware, auction documents, projects of new products, strategic plans, territorial coverage plans, marketing/ financial/ business plans, tariff plans, business projects, commercial, financial, fiscal technical regarding BRD's activity, databases on providers, information regarding BRD's relation with its providers/ suppliers, including information of any nature obtained about providers/ suppliers, information regarding BRD's relation with other entities within Groupe Société Générale and within BRD, internal normative documents, notes/minutes/other internal documents, records regarding the meetings of collective statutory bodies and/or internal committees/

other internal entities, decisions/resolutions of statutory bodies/ internal committees/ other internal entities, information which are framed in the category of privileged information in accordance with the specific regulations of capital market, databases regarding BRD's clients etc.

b) Information regarding BRD's clients – in this category are included without being limited to, the following: all facts, data, information concerning the client's person (client's name and other identification data of them) property, activity, business, business and personal relations of the clients (including financial situations of the clients, analysis files), information regarding clients' accounts-balances, flows, operations performed, attached cards etc.- to the provided bank services (bank products used by clients) and/or contracts signed with clients, as well as, any other information regarding the BRD's relation with clients.

c) Information regarding the BRD's staff – in this category are included, without being limited to, the following: any information regarding the wage, as well as, other wage rights of the employees (including potential increase or decrease of the wage), information regarding the employees' posts, hiring decisions, results of previous employment tests and examinations, information regarding the health and family of the employees, information regarding the employees' performance, assessments and training, expenses/ costs for professional development and training of the employees, the content of individual labor agreement and of collective labor agreement, as well as any information directly or indirectly received during the negotiation of collective labor agreement etc.

d) Personal data of the employees and of their family members, as well as personal data of natural persons who enter into relationship with the BRD, either as clients, customers prospects, guarantors and/or proxy of natural person clients, or as representatives/ proxy/ shareholders/ associates/ guarantors of legal person clients – in this category are included, but are not limited to, the following: first name and last name of the employees/ clients, first name and last name of family members, sex, date and place of birth, citizenship, signature, civil status data, data from driving license, number of social insurance/ number of health insurance, fix phone number, mobile phone number, fax number, address (domicile/ residence), e-mail address, work place, professional background – diplomas, studies, family situation, economic and financial situation, data bank (e.g.: card number, IBAN code), imagine, name before marriage, employee's mark, data regarding criminal record, data regarding health condition etc.

Equipment: All equipment made available to the User by BRD or personal equipment used for professional purposes (workstations, phones, tablets, etc.).
Group: Refers to the group formed by BRD Legal Person and its subsidiaries.
Information Assets: Represents all the information and/or knowledge held by the Group (including customer information, personal data, etc.).
Information System: All the elements of BRD that contribute to the creation, processing, circulation and preservation of information in the company (database, application software, procedures, documentation, etc.), including the computer system itself (central processing unit, peripherals, operating system, etc.).
Inside Information: Information of a precise nature which has not been made public relating, directly or indirectly, to issuers or Financial Instruments listed on Organised Markets within the European Economic Area (EEA), and, if made public, would be likely to have a significant effect on the prices of those Financial Instruments or on the price of related derivative Financial Instruments.
Instant messaging: Application allowing the instant exchange of messages and files between several people.
Internal community: Group of employees forming a virtual community on the communication tools set up by BRD.
IT resources: Refers to all BRD's hardware (workstations, smartphones, tablets, printers, video surveillance cameras, etc.) and software (collaborative tools, applications, etc.) that allow the User to process information in a digital, analog or paper format.

Malware: software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system such as virus, worms, Trojan horses or any other code or instruction. This software can be used to:

Infect or affect any program, software, data, file, database, computer or other hardware or component.

Damage, compromise integrity or confidentiality, disrupting in whole or in part the operation.

Hijack or allow to hijack whole or part of the Information System from the use for which it is intended to.

Personal data: Any data or information relating, directly or indirectly, to identified or identifiable individuals, irrespective of the type of information, constitutes personal data.
This applies not only to first and last names, but also to all information, which, combined with other data can be used to trace back to the person (the data subject) or to attribute the behavior of an identified group to them: contract number, address, telephone number, account number, segment, score, email, image, voice, fingerprint or DNA fingerprint, connection identifier, IP address, serial number of an electronic device, etc.
The public or insignificant nature of the data, the fact that they do not make it possible to identify individuals directly or the fact that they do not relate to their private life do not exclude the application of the law, which covers all information about an individual, irrespective of its sensitivity.
Privileged access rights: Access rights granted to certain Users allowing them extended access to the resources of the Information System, such as administrators, managers.
Security Correspondent: Security interlocutor of the Users of the Information System. Relay that makes it possible to multiply the actions of the CISO (Head of Information Systems Security) locally.
Traces: Recording memorized for all the events that occurred on an Information System level. Traces can be used for technical monitoring of applications and for investigations in order to fight against information leakage and cybercrime. The recording of the Traces constitutes an audit trail.
Users: Refers to the following natural persons who use Société Générale's Information System:

Persons involved in a service or partnership contract with BRD as well as their employees, colaborators, representatives and/or subcontractors.

In case I do not respect this Commitment, I know that it can be attracted contractual, patrimonial and/or criminal liability.

I have read, understand and respect the above,
Service Provider name: _
Name and First name: _
Date: _
Signature[2]: _

[This declaration was concluded on [date], in two copies with the same legal force, one for the Bank and one for the user[3].]
[This Declaration was electronically signed today, [date], entering into force on the date of its signing.4]

[This Annex was signed this day of [date], in two copies with the same legal power, one for each party.[5]]
[This Annex was electronically signed today, [date], entering into force on the date of its signing.[6]]

[2] *Only for the holographic signature*
[3] *Idem*
[4] *In the case of digital signing*
[5] *For holograph signing*
[6] *For electronically signing*