VERSION: July 2025

PRIVACY NOTICE REGARDING THE PROCESSING OF PERSONAL DATA

EU Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data ("Regulation" or "GDPR"), contains a series of rules aimed at ensuring the processing of personal data in accordance with the fundamental rights and freedoms of natural persons in order to increase the level of protection of personal data.
This information includes details regarding these requirements of the regulation and the way in which Banca Comerciala Intesa Sanpaolo Romania S.A. processes personal data.

SECTION 1 - IDENTITY AND CONTACT DETAILS OF THE DATA CONTROLLER

BANCA COMERCIALA INTESA SANPAOLO ROMANIA S.A. with registered office in Bucharest, Soseaua Nicolae Titulescu, nr. 4-8, America House Building, East Wing and West Wing, 6th Floor, Sector 1, Postal Code 011141, in its capacity as Data Controller (hereinafter referred to as the "Bank") processes personal data ("personal data") obtained directly or indirectly from you, including the personal data of third parties that you have provided within the framework of the existing contractual relations with the Bank, for the purposes indicated in this information. The natural persons whose data are processed by the Bank are hereinafter referred to as "data subjects".
As a personal data controller, Intesa Sanpaolo Bank Romania will always take into account that the data processing is characterized by legality, fairness and transparency, the data requested being adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

SECTION 2 - DATA PROTECTION OFFICER

B.C. Intesa Sanpaolo Romania S.A. has appointed a Data Protection Officer ("DPO") in accordance with the requirements of the Regulation. If you would like information regarding the processing of your personal data and/or the exercise of the rights provided by the Regulation, as listed in Section 9 of this information, please send a request either by e-mail: dpo@intesasanpaolo.ro or by mail to the address in Bucharest, Nicolae Titulescu Road, no. 4-8, America House Building, East Wing and West Wing, 6th Floor, Sector 1, Postal Code 011141.

SECTION 3 – CATEGORIES OF DATA SUBJECTS AND CATEGORIES OF DATA PROCESSED

A. Categories of data subjects

Depending on the business relationship and its stage of development, the Bank processes personal data of the following categories of data subjects such as, but not limited to:

- Potential customers/individual customers
- potential clients/clients who are authorized individuals (PFA),
- potential customers/entrepreneurial customers who are natural persons who own the Sole Proprietorship;
- potential clients/clients who are natural persons who independently carry out, under the law, a regulated profession;
- former customers, from any of the aforementioned categories;
- legal representatives, including guardians or curators or conventional representatives of clients in the aforementioned categories;
- legal or conventional representatives of legal person guarantors, legal person guarantors, legal person co-debtors;
- guarantors of natural persons, natural person guarantors, natural person co-debtors, natural person real beneficiaries;
- representatives;
- shareholders, associates and/or other categories of natural persons relevant in the context of the contractual relationship between a customer and the Bank, whose personal data are disclosed to the Bank directly by them or by customers, for them;

- contractual partners natural persons of the Bank or representatives or employees of the contractual partners legal persons of the Bank, etc.;
- third parties and/or legal persons/authorities and, including their legal or conventional representatives, to the extent that they have the status of litigants in the legal actions to which the Bank is a party.

B. Categories of Personal Data

Depending on the purpose and nature of the relationship, the Bank may process personal data such as, but not limited to:

- direct or indirect identification data, such as: name, surname, CNP or NIF, name of the authorized natural person and CIF, data from the content of identity documents, passport, tax residence documents provided to the Bank, citizenship, date, place and country of birth, country of residence, holographic and electronic signature, facial image (photo from the identity document, "selfie" - photo taken with the help of mobile phone/tablet, video image), this data being converted into biometric data for the verification of your identity by facial recognition technique;
- contact data (home/residence/correspondence address, e-mail addresses and mobile phone number);
- data from civil status documents, family situation, data regarding studies, professional situation, profession, occupation, position, place of work/employer's name, type of employment contract (fixed/indefinite period), date of last employment, data regarding seniority in work/seniority in the profession, public office held, political exposure (if applicable);
- economic and financial situation (income, transaction data, transaction history, relationship with other banks);
- data necessary to establish your creditworthiness, creditworthiness, ability to pay, payment behaviour, information on your creditworthiness, including your FICO score, how you meet other eligibility criteria, information on the properties you own, as well as the status of disputes;
- financial data related to the source, type, fluctuations and level of your income, bank account turnover, monthly payment commitments, garnishments or foreclosures, data about the refinanced loan, if applicable; information related to commitments recorded in balance sheet and off-balance sheet accounts (credit, similar or insurance products); information on the fulfillment or non-fulfillment of commitments to the Bank;
- data on the current situation and history of credit relations with financial, banking and non-banking institutions and information derived from them as a result of the processing carried out by financial institutions (e.g. data recorded in systems such as the Credit Bureau, the Credit Risk Center, information from public databases, etc.);
- data on fraudulent activity, data on suspicions and convictions related to crimes such as fraud, money laundering and terrorist financing (e.g. data from authorities, data from other financial institutions or from public databases such as Starbyte, World Check, the portal of the courts, etc.);
- information regarding the guarantee of your contractual obligations towards the Bank (including the identity and personal data of the guarantor, to the extent necessary for the conclusion and execution of the guarantee contract) or regarding the guarantee of the obligations of another client of the Bank (security interest, mortgage right, personal guarantee or other means of guarantee permitted by law);
- data on the beneficial owner and membership of a group of customers, participation in other companies;
- data on the banking services and products used, their accessories and data on how to access them or access the credit institution's website (purchased banking products and bank transactions, account statements, data on transaction history, guarantees offered to the credit institution, banking data such as liquidity; operating system of the device used to access online services);
- IP address of the device/equipment (e.g. mobile phone, computer, tablet, etc.) used to access the Bank's Internet and Mobile Banking services, username and other access data, access files (logs); data on geographical location, web pages visited and traffic in the Bank's applications, personal preferences and cookies);
- health data, in the case of persons who own an insurance product or request the restructuring of a credit product;
- data relating to the data subject's interactions with the Bank on social networks;
- voice and other information resulting from audio recordings, such as the recording of telephone conversations made with the Bank's staff in the customer support centers;
- information resulting from the video recording in case you visit one of our locations (territorial units or

headquarters) or use an ATM of the Bank;
- data obtained from payment instructions, data from the installation and use of the Bank's applications or special categories of personal data.

With regard to the processing of special categories of personal data (revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, and the processing of genetic data, biometric data for the unique identification of a natural person, health data or data concerning a natural person's sex life or sexual orientation) necessary to provide specific services and products, The Bank may process data such as: biometric data necessary for remote identification by video means, health data necessary either for the conclusion of an insurance product or for the restructuring of a credit product, to ensure the accessibility of the contracted products and/or services or those assimilated to social assistance services. This processing is based on the consent of the data subject, without prejudice to the specific cases provided for by the Regulation that allow the processing of special categories of personal data, without explicit consent.

C. Obtaining personal data

The Bank obtains personal data directly from the data subjects (client, proxy, legal representative, etc. at the time of filling in the requested documents/forms or using the Bank's services (e.g. Internet and Mobile Banking), or from third parties through the intermediation of information (e.g. through credit brokers/lead providers) or by querying databases/platforms or public information websites, under the conditions of the law (for example, by querying the database of the National Register for the Evidence of Persons, the ANAF database or by querying public information from websites/platforms such as portal.just.ro or RECOM) or from the Bank's customers within specific contracts for banking products/services (e.g. data of guarantors, contact persons, etc.).

D. Types of data processing

According to EU Regulation 2016/679, "data processing" means any operation or set of operations performed on personal data or sets of personal data, with or without the use of automated means, such as collection, recording, organization, structuring, storage, adaptation or modification, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

SECTION 4 - PURPOSES AND LEGAL BASES FOR PROCESSING

Purposes and legal basis of the processing

The personal data obtained by the Bank are processed as part of its activity, based on the following legal bases in order to fulfill the following purposes:

a) In order **to perform a contract to which the data subject adheres or for the actions prior to the conclusion of a contract, according to Article 6, paragraph 1, letter b of the GDPR**, the Bank processes personal data as follows, but not limited to: collecting the data of potential customers in order to initiate the business relationship; processing customer data, necessary for the steps to conclude and execute the contract, respectively for the provision of certain banking services or carrying out transactions after the initiation of the business relationship; providing the services for obtaining the qualified electronic signature certificate attached to the products and services provided by the Bank and requested by the data subjects, through the channels provided by the Bank; carrying out and authorizing trading operations, depositing/withdrawing amounts, interbank and intrabank transfers; scoring in order to contract a loan; processing data for risk analysis for the purpose of approving/rejecting decisions and, as the case may be, managing the customer relationship; operations and transactions regarding the Bank's assets and liabilities (such as, but not limited to, assignments of receivables); debt collection/debt recovery and all related activities, including contact, notification, enforcement actions; processing data representing login credentials in the applications used by the data subjects in relation to the Bank; processing in order to supply insurance products associated with specific credit products; data processing in order to carry out the insurance contracts concluded by the Bank or contracted by the client to cover various risks; sending communications and notifications regarding the performance of the banking services contract; operations of registration of movable mortgages and publicity of the related legal operations;

b) In order to **fulfill certain legal obligations/requirements incumbent on the Bank, according to art. 6, paragraph 1, letter c of the GDPR**, personal data will be processed for the following purposes, but not limited to them: the application of know-your-customer measures and measures to prevent and combat money

laundering and terrorist financing (Law no. 129/2019, NBR Regulation no. 2/2019) or the application of international sanctions, such as processing necessary for face-to-face and/or remote identification by audio and/or video means (video-selfie type, authentication on an electronic platform), monitoring the business relationship both in terms of identity verification, including by querying the databases of the National Register of Persons, carrying out and monitoring transactions, including reporting suspicious transactions to the competent authorities, consulting relevant databases, such as those managed by the National Agency for Fiscal Administration and the Credit Risk Center, RECOM, Starbyte, World Check, Dow Jones, or other similar service providers (Keysfin, ICAP, etc.), the portal of the courts, addresses and information from public authorities and institutions, etc.; taking steps to prevent and combat fraud; carrying out audit actions or reporting obligations according to the laws to various state institutions/bodies, such as the NBR, the Ministry of Finance, ANAF, ASF, CRC, including for FATCA reporting when the Data Subject is a US citizen and CRS reporting for combating tax evasion; processing data from service contracts, such as meeting legal requirements in the area of payments/payment services; processing data of third parties, from supporting documents (such as rental contracts, utility contracts) necessary to meet the know-your-customer requirements; verification and recording of the identity of visitors to financial banking units and processing of video images, in accordance with Law no. 333/2003 and Government Decision 301/2012; solving requests from competent state authorities/institutions (such as requests for information from courts, prosecutors' offices, the Ministry of Interior and other structures with attributions in this regard, such as DIICOT, etc.); managing complaints and notifications regarding banking products and/or services contracted by the data subject, as well as the data subjects' exercise of the rights regulated by the GDPR; sending notifications and information regarding the products and services owned and the business relationship or other information expressly regulated by law (such as this Information); assessment of the solvency, creditworthiness and eligibility of a client/guarantor/co-debtor in order to grant a loan; carrying out forced executions of the amounts owed as well as the administration of garnishments and seizures;

c) In order to **fulfill the legitimate interests of the Bank, based on art. 6, paragraph 1, letter f of the GDPR,** personal data will be processed for the following purposes, but not limited to them: consulting public sources, including databases with risk information, in order to ensure an optimal level of customer knowledge in order to prevent money laundering and combat the financing of terrorism, but also in order to ensure the accuracy of the data by providing by the General Directorate for Persons Records ("DGEP") the data from the identity documents of existing customers, as well as information related to the death of a customer (if applicable) through a reciprocal exchange of information by querying the DGEP database, both in order to continuously update the data on the occasion of the initiation of the customer relationship, as well as during its development, including in certain specific situations (e.g. suspicions of fraud); processing related to the management of complaints and notifications, but also for the exercise and defense of the Bank's rights in court; operations to reduce the risk of fraud by monitoring transactions, including contacting the data subjects involved; fraud prevention and investigation to prevent transactional fraud and undue payments, including by joining the SANB service (in collaboration with Transfond and other participants); data processing for statistical purposes or performing analyses based on aggregated information; processing in systems such as the Credit Bureau (in relation to which the Bank is a Joint controller); activities carried out in order to recover debts, including by using the services of a third party; consulting the records of the Trade Register in order to manage the insolvency files for individuals; processing data through market research or surveys/opinions (including second-day calls) carried out in order to improve the Bank's products and services and to optimize internal flows, policies and procedures; processing regarding the registration in contests, raffles, promotions or other similar campaigns that the Bank organizes, on its own or in collaboration with the Group to which the Bank belongs and/or with its business partners, if the eligibility criteria provided in the campaign regulations are met; processing through IT security tools (such as DLP, firewall); processing data in test environments in the process of designing, developing and using information systems, in cases where the objectives of testing are the quality and/or accuracy of the data; data processing carried out in order to optimize the flows and dedicated applications, by providing technical support and maintenance activities; audio recording of telephone conversations made by the Contact Center staff in order to solve certain requests, carry out investigations, prove a dispute, as well as to improve the quality of services; sending communications for educational and informative purposes to ensure the correct use of the owned products, reminding the facilities associated with the owned products or increasing the level of understanding on the security measures for fraud prevention (e.g. awareness card skimming messages, e-mail phishing, etc.); obtaining images or video recordings by using video surveillance systems for physical security purposes and suspicions of fraud; automated processing, without excluding human intervention, in segmentation and marketing profiling activities in order to offer personalized products or configure dedicated offers; carrying out specific reports at the level of the Intesa Sanpaolo Group that may include data on the person, property, activity, business or business relationships or with persons within the same group of customers who constitute or may constitute

a single risk, respectively on the transactions of the account(s) opened with the Bank, based on the legitimate interest, namely to ensure prudential risk management at Group level; processing carried out in the legitimate interest of Intesa Sanpaolo Bank Romania in order to carry out from a legal, technical and operational point of view the process of merger and integration of First Bank's customers and activity and to ensure the proper and continuous administration of banking products and services, ensuring the Bank's legal obligation regarding the continuity of banking services in optimal conditions. In this context, the processing of First Bank's customers' personal data during the pre-merger period is essential for aligning systems, processes, products and services, migrating customer accounts, transaction history and other important information to a unified system, ensuring a smooth transition, minimizing any disruptions and maintaining continuity of service in customer relations;

d) Based on **the expressed consent of the data subjects, according to Article 6, paragraph 1, letter a of the GDPR,** the data will be processed for the following purposes: direct marketing, as well as but not limited to: participation in campaigns and awarding of prizes, loyalty programs and special offers launched for customers, including for the promotion of any products and services of the Bank and its partners, advertising/advertising; processing data from telephone conversations made through the Contact Center service; the processing of consultation of the CRC and ANAF databases, in case of requesting a credit product; for the processing of biometric data, in the context of remote identification in order to access certain services/products of the Bank (e.g. initiation of the business relationship via internet/mobile banking, remote data updating, for enrollment for the purpose of issuing a certificate for digital signature; analysis of behavior when accessing the Bank's website, through the use of cookies, both of the Bank, and of third parties;

Automated decision-making and profiling

With regard to the creation of profiles, the Bank may carry out processing in order to evaluate your behavior. and other personal aspects. Based on this data and the consent granted, the Bank may create a profile both to identify your preferences. regarding the Bank's products, services and offers, your preferred mode of communication and your behavior. in relation to the Bank, as well as to develop new products and services. Also, some profiling activities are based on the Bank's legitimate interest, such as those of placing money laundering, terrorist financing and international sanctions at risk.
Automated decision-making processes, regulated by Article 22 of the GDPR, are those decisions taken by the Bank without the intervention of a human factor and which may produce legal effects or similarly affect you to a significant extent. In certain circumstances, the Bank may carry out such processing for purposes such as, but not limited to: verifying persons on the international sanctions lists at the time of initiating a business relationship with the Bank, monitoring transactions and adopting measures to block them depending on the amount traded or their frequency in case of identification of suspicious transactions, determining the eligibility to contract a banking product by applying an internal scoring, containing automatic eliminatory criteria (such as minimum lending criteria, degree of indebtedness, income held, FICO score provided by the Credit Bureau S.A.). Scoring is a risk assessment tool to which the Bank is exposed when granting a loan. It is based on statistical analysis, which uses your personal data and helps us determine possible refund behavior by generating a score. The score is a score resulting from the analysis of the data, which expresses the possibility of fulfilling the obligations to pay the credit installments throughout the period of the loan agreement. The Bank sets a minimum score that it accepts when granting loans, so every time the calculated score will be below the minimum threshold that the Bank has set, the loan will not be granted.

SECTION 5 - OBLIGATION TO PROVIDE PERSONAL DATA

The personal data are provided to the Bank by the data subject or authorized persons upon request for the products/services provided by the Bank within the specific documents, and in relation to them, the refusal to process the data, expressed at the initiation of business relations, will make it impossible for the Bank to follow up on requests for such products or services. Also, after the conclusion of contracts with the Bank, the periodic provision of updated data is necessary for their performance and the fulfillment of the legal obligations and legitimate interests of the Bank.

SECTION 6 - CATEGORIES OF RECIPIENTS

In order to achieve the purposes indicated above, depending on the customer relationship and the products or services purchased, the Bank may transmit your personal data to the following categories of recipients:
a) the data subject and/or his/her legal or conventional representatives;
b) third party contractors and contractual partners of the Bank from all areas necessary for the optimal performance of the Bank's current activity (e.g.: insurers, debt collection agencies, lawyers, notaries, bailiffs,

appraisers, auditors, consultants, companies in the IT/payments area, providers of fraud investigation and documentation services, postal and courier services, IT service providers, archiving services in physical and/or electronic format);
c) partner banks and correspondent banks, banks or financial institutions participating in syndicated loans and other financial entities/payment service providers, including PSP third parties (such as payment initiation service providers, account information service providers, and payment service providers issuing card-based payment instruments) to perform certain payment services and cash withdrawals;
d) providers of technical services for processing and facilitating inter-bank payments (e.g. Nexi Croatia, Transfond, SWIFT, Bucharest Stock Exchange), providers of payment instrument production and personalization services, providers of technical payment facilitation services (such as Visa and Mastercard), providers of payment initiation services and providers of account information services;
e) trusted service providers (such as Onfido, CertSign) in order to identify, authenticate you and for generating the electronic signature certificate;
f) providers of market research services/media agencies, providers of transmission of communications of any nature, including legal/contractual or marketing;
g) if you have contracted credit products, the data may be transmitted to database organizing offices, such as the Credit Bureau, the Credit Risk Center, the Payment Incidents Center, but also to entities with a guarantor role, such as FNGCIMM, the Rural Credit Guarantee Fund, APIA, IDB or public authorities and institutions such as the National Agency for Cadastre and Real Estate Advertising ("ANCPI"), National Register of Publicity of Security Interests ("RNPM");
h) the Data Subject's employer;
i) companies within the Intesa Sanpaolo Group, both to the parent company and to other subsidiaries or entities within the Group, including companies offering IT, administrative and/or financial services;
j) Shareholders;
k) entities with which the Bank has concluded financing agreements or assignments of receivables, third parties in the case of assignment/transfer of the Bank's rights;
l) state authorities, according to their competences and the applicable legislation, and public information systems set up at the level of public administrations/authorities, such as: the National Bank of Romania (NBR), ASF, the National Authority for Consumer Protection - ANPC, the National Office for the Prevention and Combating of Money Laundering - ONPCSB, the National Agency for Fiscal Administration (ANAF), the National Supervisory Authority for Personal Data Processing - ANSPDCP;
m) ANAF - in order to comply with FATCA ("Foreign Account Tax Compliance Act") and CRS (Common Reporting Standard) legislation, if the personal data or operations performed by you fall within the reporting criteria established by FATCA and/or CRS;
n) National House of Public Pensions, Ministry of National Defense, Ministry of Internal Affairs, County Agencies for Payments and Social Inspection (for the delivery of pensions, allowances and/or other allowances);
o) judicial/investigative and control authorities, judicial authorities, central and local public authorities;
p) any other categories of contractual partners necessary for the performance of the Bank's current activity.

SECTION 7 - TRANSFERS OF PERSONAL DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS OUTSIDE THE EUROPEAN UNION

Personal data may also be transferred outside Romania, both within the European Economic Area (EEA), in countries such as Italy, Croatia, Hungary, Germany, Ireland, and outside the EEA, including the United States of America and the United Kingdom of Great Britain.
The Bank will ensure that the transfer, as appropriate, of personal data outside the EEA meets an adequate level of protection similar to that within the EEA, either through standard contractual clauses adopted at the level of the European Commission (together with other additional safeguards, where applicable) or other safeguards recognised by law (such as adequacy decisions – as is the case with the transfer of data to the United Kingdom). The Bank will not disclose personal data to parties who are not authorized to process them.

SECTION 8 - RETENTION PERIOD OF PERSONAL DATA

Your personal data Personal data is processed using manual, electronic and automated tools and in a manner that ensures its security, confidentiality, integrity and availability.
Your data. are kept for a period that does not exceed the period necessary to achieve the purposes for which they are processed, without prejudice to the storage conditions imposed by law. For example, but not limited

to:

- your personal data is kept for a period of 10 years from the date of termination of the contractual relationship or for a period of 6 months if a contractual relationship is not concluded between you and the Bank (unless a longer retention period is required or provided for by law);
- the personal data transmitted to the Credit Bureau S.A. are stored for a period of 4 years from the date of the last update;
- the personal data transmitted to the Credit Risk Center are stored by it for 7 years from the date of registration;
- the video recordings will be kept for a maximum period of 30 days, unless there are good reasons for keeping them for a longer period;
- the personal data processed for direct marketing purposes will be kept as follows: a) for a period of no more than 3 years from the moment of termination of the contractual relations concluded with the Bank, if you have become a customer of the Bank or b) for a period of no more than 3 years from the moment of granting consent, if a contractual relationship is not initiated between you and the Bank.

It is possible that, following the fulfillment of the legal archiving deadlines, the Bank will order the anonymization of the data, thus depriving them of their personal character and will continue the processing of anonymous data for statistical purposes.

SECTION 9 - RIGHTS OF THE DATA SUBJECT

As a data subject, you have the following rights:

1) **the right of access**, **the right to information**: the possibility to be informed if and what are the personal data we hold about you, access to them and to information such as: the purposes and duration of the processing, the source of the data, the recipients or categories of recipients to whom the personal data have been or are to be disclosed, etc.;

2) **the right to rectification**: the possibility to request the updating, completion or correction of the data relating to you, so that they are always accurate;

3) **the right to erasure ("right to be forgotten"**): the possibility to request the deletion of your data if certain conditions are met, in accordance with the legal provisions. We inform you that the Bank cannot delete your personal data if their processing is necessary, for example, to comply with a legal obligation, for reasons of public interest, to formulate or exercise legal action;

4) **the right to restriction of processing**: the possibility to obtain from the Bank the restriction of the processing of personal data, in certain situations, such as: the data subject contests the accuracy of the data or the lawfulness of the processing, the data subject opposes the deletion of the data, when the Bank no longer needs the personal data for the purpose of processing, but the data subject requests them for ascertainment, exercising or defending a right in court or then the data subject opposes the processing, for the period of time in which it is verified whether the legitimate interests of the Bank prevail over those of the data subject;

5) **the right to data portability**: if the processing of your personal data is based on consent or is necessary for the performance of a contract or in the context of the steps taken to conclude one, and the processing is carried out by automated means, you may: request to receive your personal data provided in a structured, commonly used and machine-readable format; transmit this data to another controller, without hindrance from the controller to whom the personal data has been provided. You also have the right to request that your personal data be transmitted by the Bank directly to another data controller indicated by you, if this is technically possible for the Bank. In this case, you will provide the Bank with the exact details of the new data controller to whom you intend to transmit them and you will provide the Bank with a written authorization in this regard;

6) **right to object**: at any time, you have the right to object to the processing of your personal data if the processing is carried out for the purpose of performing a task performed in the public interest or is necessary for the purpose of the Bank's legitimate interest (including profiling). If you decide to exercise this right, the Bank will no longer process your personal data, unless it demonstrates that it has legitimate and compelling reasons or legal obligations that justify the processing and that prevail over the interests, rights and freedoms of the data subject or that the purpose is to establish, exercise or defend a right in court;

7) **Automated individual decision-making, including profiling**: The Regulation grants the data subject the right not to be subject to a decision based solely on automated processing of personal data, including profiling, which may produce legal effects concerning the data subject or similarly affect him or her to a significant extent, unless the above-mentioned decision: a) it is necessary for the conclusion or execution of a contract between the data subject and the Bank; (b) is authorised by Union or national law applicable to the Bank; c) is based on the explicit consent of the data subject. In the cases referred to in points (a) and (c), the Bank

shall implement appropriate measures to protect the rights, freedoms and legitimate interests of the data subject, at least his or her right to obtain human intervention from the controller, to express his or her views and to challenge the decision. In this regard, the data subject must submit to the Bank a request requesting the intervention of a human operator, expressing his point of view and contesting the decision, to the contact details mentioned in this Notice;
8) **The right to lodge a complaint with the competent supervisory authority** for data protection: without prejudice to the right to appeal to any other administrative or jurisdictional court, if you consider that the processing of your personal data takes place in violation of the Regulation and/or the applicable regulations, you may file a complaint with the National Authority for the Supervision of Personal Data (official website: www.dataprotection.ro).

You can exercise these rights at any time by sending a request or you can address any questions or concerns regarding the processing of personal data to the e-mail address dpo@intesasanpaolo.ro, by mail to the headquarters of B.C. Intesa Sanpaolo Romania S.A. in Bucharest, Nicolae Titulescu Road, no. 4-8, America House Building, East Wing and West Wing, 6th Floor, Sector 1, Postal Code 011141, or directly in any of the Bank's territorial units.
The Bank will manage and respond to your requests in relation to the exercise of the above-mentioned rights free of charge and within the term provided by the legislation in force, but it is entitled to charge a fee or refuse to comply with your requests if they prove to be excessive or unfounded.

The Bank has the obligation to provide information on the actions taken as a result of the exercise of the above-mentioned rights, without undue delay and, in any case, within one month from the receipt of the request. In the case of complex or very large applications, this deadline can be extended by two months. In this case, the Bank has the obligation to inform the data subject about such an extension, within one month from the receipt of the request, also presenting the reasons for the delay.

This information is updated periodically and can be consulted at any time on the official website of Banca https://www.intesasanpaolobank.ro/, Data Protection section.