Nexent Bank's Privacy Policy

We understand your concern regarding how your personal information is used.

This notice outlines **Nexent Bank N.V.**'s ("**Nexent Bank**" or "**the Bank**") approach to privacy and the management of personal data ("Data").

As of May 25, 2018, the latest European regulation on personal data protection came into effect: Regulation (EU) No. 679/2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, repealing Directive 95/46/EC (the "General Data Protection Regulation" or "GDPR" or "the Regulation").

We want to reassure you of the importance we place on safeguarding your Data and complying with security obligations. We also wish to inform you about the rights you hold under the new Regulation.

Please find below details on the following questions:

- Who are We?
- To WHOM do we address this Policy?
- What DATA do we process?
- WHY do we process data?
- IF we process data automatically
- With WHOM do we share data?
- HOW LONG DO WE KEEP THE DATA?
- The implications of refusing to provide DATA
- Processing data outside the European Economic Area (EEA)
- What can you do to help us keep your data safe
- The rights of the data subjects
- How to contact us. The data protection officer
- Changes to this Policy

➢ WHO ARE WE?

Nexent Bank N.V. is a credit institution registered in the Kingdom of the Netherlands (the Netherlands) – a member state of the European Union, with its registered office in

Amsterdam, 6A Karspeldreef, 1101 CJ Amsterdam, Netherlands, telephone +31 (0)20 35 76 300, e-mail info@nexentbank.nl, registered in the Trade Register at the Dutch Chamber of Commerce under no. 33256675, supervised by De Nederlandsche Bank, the National Bank of the Netherlands, with postal address Postbus 98 1000 AB Amsterdam, telephone +31 20 524 9111, e-mail info@dnb.nl ("DNB") and registered in the register of credit institutions kept by it under no. B0546, through **Nexent Bank N.V. Amsterdam Bucharest Branch**, headquartered in Bucharest, Timișoara Boulevard, no. 26Z, Anchor Plaza Building, sector 6, postal code 061331, e-mail office@nexentbank.ro, registered with the Trade Register Office under no. J2024027422009, unique registration code 50637620, European unique identifier (EUID) ROONRC.J2024027422009, entered in the Register of Credit Institutions with number RB-PJS-40-079/11.11.2024.

In Romania we own the following sites: www.nexentbank.ro, www.cardavantaj.ro, www.optimocard.ro.

➢ TO WHOM DO WE ADDRESS THIS POLICY?

In essence, we process personal data for the purpose of providing services and delivering financial-banking products, conducting a prudent and healthy banking activity, in a highly professional manner, in this respect observing the regulations, the commitments to which the Bank is a party or which are applicable to it, as well as the codes of conduct, industry practices and standards, in accordance with the requirements of the General Data Protection Regulation no. 679/2016, as well as the other applicable regulations related to data processing and protection.

The specific terms related to the organization, functioning, activity of a credit institution, as well as to the financial-banking products and services whose meaning is not defined in the General Business Conditions or do not result from this document will be interpreted according to the applicable regulations and / or banking industry norms. In this regard, the Bank will furnish additional details or explanations upon the client's explicit request.

Personal data processed by the Bank belong to the data subjects, such as: individual clients, authorized individuals or individuals conducting activities independently in any of the forms prescribed by law, individuals associated with corporate clients (such as shareholders, directors, administrators, delegates, employees, and any other individuals representing the client in their relationship with the Bank, including the individuals holding such capacities for the administrator, the legal administrator, the liquidator or the legal person representatives of the client), the legal, conventional or authorized representatives of the client, the real beneficiaries, co-debtors, guarantors, additional users, contact persons, as well as the family members of some data subjects (such as the individual client), the natural persons whose data are provided in documents made available by or for clients, other persons who use or benefit in any way from the services

of the Bank, the beneficiary of a payment operation, the beneficiary of an insurance, persons subject to the garnishment procedure, visitors of a website belonging to the Bank or visitors of the physical locations of the Bank. These personal data are included in the documents and / or information obtained / received by the Bank, directly from the client or from any other individual or legal persons in compliance with the law, in order to initiate business relations with the client, regardless of whether a transaction / relationship negotiated or discussed with or for the client is completed or not, as well as during the course of business relations with the Bank.

At the same time, individuals who interact or communicate with the Bank as representatives (in a broad context), employees, delegates or consultants of the Bank's partners hold the status of data subjects. The Bank receives or obtains their personal data during the negotiation, conclusion and ongoing development of business relations with these partners, including, without limitation, service providers, consultants, experts, partners in business projects, sponsorships beneficiaries, etc.

In certain situations, in order to initiate and carry out various business relationships with the client, the Bank may process personal data belonging to certain categories of data subjects (for example, real beneficiaries, delegates, spouses, persons whose incomes are analyzed in order to be taken into consideration when granting products / services by the Bank, the recipients of payments ordered by clients, clients of the Bank`s clients, including assigned debtors or debtors of mortgaged receivables) without benefiting from the practical method of directly ensuring the information of these categories of persons or even without being able to ensure full confidentiality of the relationship with the client at the same time. In this regard, it is the responsibility of the client to ensure that he/ she has properly informed the data subject about the processing of his data according to this document as well as to obtain his express consent, to the extent that this consent is requested by the Bank as necessary according to the applicable legal provisions.

We may also process your Data even if you do not have a connection with Nexent Bank. For example, surveillance cameras may capture your image when you visit our premises. Details can be found in the sections below. Or some authorities (courts, notaries, tax authorities, criminal investigation bodies, etc.) may send Bank requests and documents containing your identification data (such as, for example, unavailability or enforcement measures, requests to provide information, etc.).

We intend to inform you through this document about the processing of Data, which we perform if you visit Nexent Bank’s websites or offices, enter into dialogue with us in order to purchase banking products or services, if you are already our client or you have a relevant relationship in relation to the products or services offered by the Bank to a client or potential client (co-debtor, guarantor, representative, etc.) or you have or want another kind of collaboration with us, directly or for someone else. Under the same

conditions, we will carry out the processing of personal data as a data processor on the basis of mandate or service provision relationships, and with regard to the data of the data subjects who have a legal relationship with another entity from the Nexent Bank group and who processes data as a data controller.

If you want to know how we process your Data when you visit our websites using cookie modules, see our section dedicated to the Cookies Policy.

If you are in a recruitment process with us, please see the Careers section.

Whenever you visit the Bank's units or use its ATMs, please also consult the additional information made available locally regarding data processing through the video monitoring system.

Also, at the time of data collection, if and to the extent necessary in addition to the provisions of this policy, the Bank will inform the client to what extent the data collected is necessary to provide a product or service or for compliance with a legal or contractual obligation, as well as regarding the possible consequences of non-compliance with this obligation.

➢ WHAT DATA DO WE PROCESS?

We process personal data as a data controller, directly, but also through processors, such as subcontractors of various services. Also, the Bank can process data together with other parties having the quality of joint controllers, for example, in the case of co-branded cards, insurance products, within the relationship with Credit Bureau or together with other contractual partners who hold the status of data controller, such as other financial institutions involved in the execution / settlement of operations instructed by the client or in the performance of other services.

a) Identification and contact data, necessary for the purpose of identification and communication to initiate, negotiate and carry out contractual relations until all their effects are extinguished, including for the collection of debts:
    - name, first name, nickname, personal identification number, identity document serie and number, passport number, driving license, social or health insurance number; the image and the other data contained in the identity documents, the security question in relation to the Bank (for example: mother's name before marriage), biometric data (based on facial image and voice) used for the purpose of unique identification through the use of audio/video means of communication and remote identification, citizenship, home address, residence and correspondence address, telephone number and other contact data for distance communication means, IP address (internet protocol) of an electronic device, the

holographic signature, the electronic signature, unique identification codes in relation with the Bank (for example: client code, user, passwords declared for identification in case of telephone contact), the current account number (IBAN), authentication codes (in the context of payments by electronic means such as internet and mobile banking);

b) Data and information of a financial nature, necessary mainly for the purpose of evaluating the granting of credit products and the development of the credit relationship:
   - profession, place of work, position held, professional qualifications, family situation (to determine co-debtors or dependents for the purpose of credit risk assessment), types and levels of income and expenses, criminal record or tax information (for example, in the context of credit relationships, litigation), solvency, information related to credit history, utilities / telephony or insurance, any other information made available by entities such as the Credit Bureau SA or the Central Credit Register, the National Agency of Fiscal Administration, data made available by public registers such as the National Trade Register Office, the Land Book Office, the National Movables Publicity Register or publicly available data in mass media, the Internet or on professional or social networks;

c) Data and information required for the purpose of providing the services by electronic means, online or by telephone or to ensure the security and fraud prevention requirements:
   - information related to the location of transactions through electronic payment instruments or with remote access, voice, image and information contained in audio or video recordings of communications by distance means (to improve the quality of services and to provide proof of requests / agreements / the options thus expressed by or for the client) as well as in the recordings related to the video surveillance means used at the Bank's premises or at the ATMs (for security reasons and fraud prevention),
   - public office held or public or political exposure, relationship with entities in the Bank's group, information regarding the fraudulent / potentially fraudulent activity of the data subjects (for processing in accordance with the law requirements for fraud or money laundering prevention and terrorist financing combating through the banking system),
   - information related to the inadvertencies found in the documents / statements presented to the Bank, obtained on the basis of the forms, declarations and documents of any kind submitted to the Bank or obtained by it from any sources allowed contractually or under the law or related to the Beneficiary Name Display Service (SANB) (service offered in collaboration with Transfond and the other participating banks) and the similar SANB service developed and implemented by the Bank for intra-

bank payments in lei (payments towards Nexent Bank customers), in order to prevent transactional fraud and undue payments (made by mistake to other beneficiary than the one initially intended);

d) Other personal data and information:
   - data obtained through operations of combining, segmenting, organizing or extracting the above data,
   - any other categories of data that the client provides to the Bank or that it acquires and processes in compliance with the law or the applicable contracts for the relationship with the client;
   - data regarding operations carried out through internet/mobile banking applications and/or other banking applications (logs, diaries, time stamps, etc.).

e) Special categories of data:

The Bank does not process special categories of data in the normal course of its dealings with the Customer or other data subjects. However, the Bank may process, in compliance with the obligations and legal and contractual guarantees of the Bank, data on the health status in the context of the services offered regarding insurance policies related to the services and products contracted by the Bank or offered by the Bank as an affiliated agent - secondary intermediary for insurance products or in the context of providing facilities at the client's request (for example, credit restructuring, payment commitments). The Bank may also process special data insofar as it is included by the Data Subject in the details provided to the Bank upon the provision of services by the Bank (for example, explicit details contained in Customer's Payment Instructions).

In order to fulfill the purposes mentioned in this section, the Bank processes personal data acquired either directly from the data subject or indirectly from interactions with other persons directly related to the data subject, depending on the concrete relationship between them, as shown by the above explanations. Additionally, including on the basis of the processing of the data thus obtained, the Bank may generate (for example, codes or customer identifiers) or infer (for example, the degree of solvency) new personal data or may acquire / receive data from external sources, such as:

- **institutions, public authorities or other entities that manage publicly available or restricted access databases**, in particular: the General Directorate for Personal Records - DGEP, National Agency for Fiscal Administration - ANAF, the National Credit Guarantee Fund for Small and Medium Enterprises – FNGCIMM, relevant entity for example in the case of First House type loans, the Central Credit Register - CRC or the Payment Incident Register - CIP organized by the National Bank of Romania, the

Trade register, the portal of the courts, the Credit Bureau, the national notarial registers, official databases with persons subject to international sanctions in the matter of preventing and combating money laundering and terrorist financing or from any other credible and independent sources (such as databases of public sector bodies or private databases containing information from public authorities, audit reports, tax documents, bank statements, etc.) etc.;

- **entities involved in the execution of payment operations or in the operation of payment instruments,** such as: international card organizations (Mastercard, Visa), economic operators that accept payment by cards or other remote payment instruments, banks and other payment institutions involved in payment schemes, Transfond, SENT, Regis, Central Depository, SWIFT etc.;
- **business partners**, such as collaborators or service providers for the Bank, as well as entities to which the Bank provides payment services, securities issuers, insurance companies, random other legal person from which the Bank may acquire receivable rights in relation to the clients etc;
- **online platforms** accessible to the public, including social and professional networks, Internet networks;
- **other entities from the Nexent Bank Group**;
- **employers of the data subjects, partners or counterparties of the client,** who make payments of salaries or other income to the client or request payment from the client's accounts under automatic debit arrangements (direct debit).

➢ WHY DO WE PROCESS DATA?

The processing carried out by the Bank for the purposes detailed below is primarily required for the Bank's compliance with its legal obligations or the execution/ preparation of a contract which the Data Subject is/ will be a party to. At the same time, however, the Bank has a legitimate interest in ensuring the best quality standards, prudence and professional diligence, in order to be able to fully carry out the activities that are allowed by law, to develop and carry out business strategies, so as to constantly meet the expectations and needs of its clients and to adapt to the requirements, trends and evolution of the market not always preceded by express legal regulations, in order to maintain its competitiveness in the market, the Bank needs to process personal data based on its legitimate interest, the related data processing not always being limited to express legal texts or contractual clauses.

Therefore, with regard to a certain purpose, depending on its broader or narrower formulation and interpretation, the processing basis for the various actual activities it implies may be cumulated. Before any processing, however, the Bank analyzes its validity

in accordance with the principles of the General Data Protection Regulation (GDPR), always ensuring the existence of the legal basis and compliance with the conditions imposed by the regulations in force for the legality and security of the processing of personal data.

The Bank processes the data and information of the data subjects, necessary for **entering into a contractual relationship and the execution of contracts** concluded with the data subject and for the purpose of providing the products and services to the customer, carrying out processing in this respect mainly for the purpose of:

a) assessment of eligibility for the provision of standard or customized banking products and services (including in the approval / granting stage) or for accepting requests for restructuring, rescheduling, etc.;
b) the performance of any legal relations between the Bank and the data subject deriving from the current account relationship or from another special contract concluded between the Bank and the data subject, including through the use of advanced or qualified electronic signatures, in order to provide financial - banking services;
c) managing of the relationship with the data subject, including any subsequent changes regarding the characteristics, terms and conditions of the product or service;
d) execution of banking transactions in good and safe conditions, by any means of instruction: at the counter, Internet, card (physical or virtual), POS (physical or virtual, including through contactless technology, NFC/ near field communication) etc.;
e) monitoring of all the obligations assumed by the data subject towards the Bank or other entities from its group;
f) debt collection / receivable recovery (as well as activities preceding them);
g) conclusion and / or execution of insurance and reinsurance contracts (including for the situation in which the data subject, as an insured, benefits from insurance in case of occurrence of the insured risk);
h) establishing, exercising or defending some of the Bank's rights in court or in relation to other authorities;
i) management of requests / complaints / claims / petitions / investigations regarding the Bank's activity and its services or products;
j) performing and processing the payment operations through the SWIFT system or facilitators of online card payment services, or providing services related to the use of cards or virtual POS, if applicable;
k) necessary exchange of information in order to issue and use by the client the cards (physical or virtual) issued by the contractual partners Visa and MasterCard, as well as to make payments through virtual POS or through "contactless" technology (contactless or NFC/near field communication);

l) use of simple, advanced or qualified electronic signature in the relationship between the Bank and the Client;
m) communication with the data subject for the fulfillment of any of the above purposes, by using any contact details.

The Bank processes personal data necessary **to comply with its legal obligations**, carrying out processing in this respect mainly with the purpose of:

a) identifying and knowing the clientele, preventing money laundering and combating terrorism financing, preventing fraud and guaranteeing bank secrecy, including through the collection in the computerized system of the data contained in the client's identity documents, of the biometric data contained in the registrations relating to the remote identification by video means (including through authorized providers), as well as other data regarding the quality of the client or the family member of the publicly exposed person ("PEP"), belonging to a group of clients, source of funds, other data included in the contracts concluded with you or results during the execution of the contract;
b) guaranteeing the legal rights of the client / data subject in relation with the Bank, regarding the information, the services provided and the data processing carried out by it or in connection with the provision of services through third party payment service providers;
c) fulfillment of the fiscal obligations, including regarding taxes and withholding taxes;
d) provision of reports and information at the request of the authorities (for example, courts, research bodies, law enforcement bodies, foreclosure bodies, public notaries, tax authorities);
e) enforcement of court decisions and other orders of the authorities (for example blocking of accounts by garnishment, establishment of insurance measures);
f) managing conflicts of interests;
g) management of audits, controls and investigations by local, European or parent company supervisory authorities (for example, the National Bank of Romania, the Central Bank of the Netherlands, the competent tax authorities, the consumer protection authority, competition supervision authority, authority for supervision of personal data processing);
h) management of statutory, internal and external audits;
i) ensuring the security in the Bank's premises, its territorial units and ATMs;
j) credit risk management and risk management by creating risk profiles;
k) client portfolio management and financial administrative management;
l) meeting the prudential reporting requirements at group level and of transaction reporting requirements in relation to the supervisory or fiscal authorities;
m) keeping / depositing /storing and archiving (physical or electronic) documents (physical or electronic);

n) implementation of personal data security measures and business continuity management in the event of unforeseen situations, including by making backup copies;
o) implementation of means that allow any person to report the inconsistencies detected in connection with the banking services offered by the Bank;
p) assessment and management at the consolidated level, of the financial group, of the risks specific to the activity carried out, in accordance with the European and international regulations, regarding the minimum capital requirements, the supervision of the capital adequacy and the market discipline of banking institutions;
q) fulfilling the reporting and/or information analysis obligations in accordance with the international conventions to which Romania or the Netherlands are party, such as FATCA and CRS, as well as fulfilling the reporting and information analysis obligations highlighted in the Central Credit Risk database, at the initiation and during the management of the contractual relationship;
r) the use of advanced or qualified electronic signatures, in the relationship between the Bank and the Client;
s) communication with the client/ data subject for the fulfillment of any of the above purposes, by using any contact details.
t) for compliance with the legal obligations of the merging companies, in the context of the merger operations in which the Bank is involved, for example in connection with the receipt and processing of observations sent to the Bank regarding the merger project.

In **pursuit of the legitimate interests** that the Bank has in relation to the proper management of its activity as detailed above, the Bank performs personal data processing mainly for the purpose of:

a) improving the quality of the services provided by streamlining flows, optimizing costs, training of employees, improving customer response times, including by creating and managing internal databases, processing data regarding customer preferences;
b) design, development, testing and use of IT computer systems and services (including database storage / archiving, in the country or abroad);
c) diversification of products and services and their adaptation to clients needs, business planning;
d) maintaining the reputation, integrity and security of the business, resources and equipment;
e) liquidity management, balance sheet optimization;
f) archiving in physical and / or electronic format of the documents for their efficient access and management;

g) marketing activities, including the transmission of advertising materials not directly addressed, as well as conducting surveys regarding the services offered by the Bank and its activity;
h) business administration, including through the alienation / transfer or acquisition of assets, mergers, acquisitions, transfers, sales/purchases of portfolios of contracts, receivables or parts of the business, or through other similar transactions, carried out both with entities from the Bank group (such as Nexent Bank), as well as with any other interested parties, which may include the disclosure of any information and data relating to the Bank's clients/data subjects for the conduct of negotiations or evaluations (due diligence) by persons interested in carrying out such transactions, as well as in general in the context or with a view to concluding, implementing or executing certain such transactions, but also the collection of identification data and related to the capacity in which the person acts, provided directly by him or by his powers of attorney, in order to verify that the comments regarding the merger project are received from the persons who have the legal right to formulate them, with the application by the Bank of appropriate measures to guarantee the rights of the clients/data subjects in the context of these operations;
i) analysis of preferences by reference to the products and services contracted from the Bank, from other entities in the group or from other financial service providers (according to the data obtained from consulting external databases such as the Credit Bureau, etc.), analysis of solvency, the credit risk and / or other details regarding the history and characteristics of the transactions, to the extent that such profiling does not produce possible legal effects or a similar significant impact, in order to promote other products and services offered by the Bank, designing dedicated or exclusive services and products, as well as for credit risk assessment;
j) identification of the goods and the updated contact details of the client / data subject bound to the Bank, in order to exercise the Bank's rights regarding the recovery of debts;
k) fulfillment of the obligations assumed by the Bank by adhering to the system rules of the card service providers, of the clearing-settlement institutions, to international practices and usages;
l) data processing for statistical and research purposes, to understand customer behavior and preferences, to identify and manage operational risks, to optimize flows;
m) transmission and reception in relation to entities such as the Credit Bureau, the Central Credit Register, the Payment Incident Register of the credit or payment risk information registered in the name of the relevant client / data subject (for example, the credit risk situation and the status of outstanding loans, as well as information about the credit products, or other commitments from which the

relevant client / data subject benefits), in order to initiate or carry out credit relations with the client or to issue credit or payment securities (bills of exchange, promissory notes, checks, etc.);

n) communication with the client/data subject for the fulfillment of any of the above purposes, by using any contact details.

o) prevention of fraud or erroneous transactions in the online environment. For this purpose, the Bank processes certain personal data of its customers (full first name, initial of the name and IBAN codes of the accounts held by the customers) to offer the Beneficiary Name Display Service (SANB) managed in collaboration with TRANSFOND and other participating payment institutions. The personal data thus transmitted by the Bank to TRANSFOND are stored and updated by it periodically until the termination of the business relationship with the Bank. At the same time, the Bank, as an independent data controller, processes the same personal data as those mentioned above to provide a similar service to SANB, developed and implemented by the Bank for intrabank payments in lei (payments to Nexent Bank customers).

p) verifying, correcting, completing and updating the Client's data, in order for the Bank to comply with its obligations derived from the regulatory framework applicable to the financial-banking field and the principles/customs related to it, as well as for the purpose of pursuing its legitimate interests.

To the extent that, according to the laws, the consent of the data subject is necessary, the Bank will obtain such consent on the initiation of the business relationship with the client / data subject or later, by means such as completing and ticking the Bank's forms when requesting a product or service, signing information notes or through the Bank's website or online banking applications such as internet banking, mobile-banking or related to other services and products offered by the Bank. Most likely, the Bank performs personal data processing based on consent for purposes such as:

a) direct transmission of advertising messages by email, SMS or other means that does not involve a human operator, in order to promote the most suitable products and services of the Bank or to promote the services of other entities in the group or of contractual partners outside the group;

b) in-depth analysis by automated means, including through the use and combination of several data such as those regarding the history of transactions, their characteristics, the location of the transaction initiation, other data obtained by consulting internal and external databases and / or online platforms (for example, regarding the credit history, the history of the relationship with the Bank or entities in its group, etc.) and the creation of profiles in order to customize dedicated and exclusive offers, to the extent that, according to the applicable regulations, the consent of the data subject is required by reference to the possible legal effects or have a similar impact in a significant manner;

c) analysis of the person's behavior when accessing the Bank's website, through the use of cookies, both of the Bank and of third parties (information about the Bank's Cookies Policy can be consulted on the Bank's website http://www.nexentbank.ro/politica-de-cookies/).
d) remote identification of the person through the use of photo/video means in order to remotely conclude contracts such as credit cards, debit cards, current accounts, overdrafts, other loans for personal needs, as well as updating customer's personal data.

The consent expressed with regard to data processing based on the consent of the data subject can be withdrawn at any time, without affecting the legality of the processing carried out before the withdrawal, the information of the data subject regarding the said processing or the legality of the processing that is based on another legal basis as it appears from this section. Likewise, the withdrawal of consent will not affect the provision by the Bank of the contracted products or services. However, it is possible that in the future we cannot keep you updated with the latest offers, respectively that we will not be able to communicate personalized offers. When collecting the consent, the Bank will provide the data subject with additional information on the purpose of the data processing, the possibility of transferring it to third parties, as well as regarding a simple way to withdraw it.

Processing for further purposes

The Bank will process personal data also for other purposes in relation to its legal obligations or future legitimate interests. The client has access and can check at any time additional updated information regarding the categories of data, the purposes and grounds of the processing, the categories of recipients of the data through the confidentiality policy in the version available on this website, at the Bank's offices or provided on request in paper or electronic form.

It is possible that, after the fulfillment of the processing purposes, after the fulfillment of the legal archiving terms or following the request to delete the data, the Bank may order the anonymization of the data (thus removing their personal nature) and continue the processing of anonymous data for statistical purposes.

Direct marketing and commercial communications

As detailed above, it is the legitimate interest of the Bank to further promote its products and services to the client, being able to do so by sending commercial materials through courier / postal services or through phone calls with a human operator. At any time during the relationship with the Bank, the data subject has the right to refuse the processing of his/ her data for direct marketing purposes, by exercising the right of opposition, according to the details offered in the section below – The rights of the data subject.

Also in its legitimate interest, the Bank may use the e-mail address obtained directly from the data subject when selling a product or service to him/ her, as well as banking applications such as internet banking, mobile-banking, in order to make commercial communications regarding similar products or services offered by the Bank. In all these cases, the data subject will have the opportunity to object simply and free of charge, both at the time of providing the e-mail address and at any time thereafter.

➢ IF WE PROCESS DATA AUTOMATICALLY

In compliance with the appropriate legal basis, the Bank may use automated individual decision-making processes, including as a result of profiling and which in certain circumstances may produce legal effects on the data subject or similarly significantly affect him/her, for example, by refusing to execute the Customer's instructions, refusing or restricting access to the Bank's products and services (by blocking a suspicious or erroneous transaction, blocking the card or account, etc.). Profiling involves the automatic processing of the Customer's/data subject's data in order to analyze and/or evaluate various aspects related to him/her, such as: transactional behavior and preferences, degree of indebtedness, inclusion on various public lists of domestic and international sanctions related to the financing of terrorism and money laundering, suspicions of fraud, etc.

Thus, the Bank has strict **legal obligations** regarding the identification of clients, the prevention of money laundering, fraud and terrorism financing. The Bank can carry out automatic processing in order to verify suspicious transactions or to identify transactions that may be subject to international sanctions. In this regard, the Bank verifies databases that include persons subject to such sanctions or who are at high risk of fraud, refusing business relations or certain transactions with the client / other data subject as a result of such verifications. Also, in order to comply with the legal obligations regarding the security of the payment instruments, but also to ensure the proper execution of the contract, the Bank monitors the payments made with its card or online through other payment instruments with remote access and adopts automatic protection measures, such as blocking the payment instrument or the account, restricting the transaction, in case of identifying some operations that do not correspond to the customer's transactional profile (such as, for example, unusual repetitive payments in terms of frequency, value, etc. or other transactions with illogical sequences by reporting at time and location).

In order to remotely **conclude a contract** with the Client or to execute a remote instruction from him, the Bank uses video means for remote identification or means for remote authentication of the Client's identity, these presuppose data processing and issuing automated decisions regarding the identification of the Client and the analysis of his request/instruction. Remote identification by electronic means, including video,

always involves the processing of the data subject's biometric data and/or voice, and in the absence of consent in this regard, the Bank will not be able to offer products and services remotely. In order to initiate a relationship and/or identify the Client remotely, the Bank may perform data processing and issue automated decisions in relation to the identification of the Client. Client requests made by remote means may be rejected if the algorithms and criteria used by the Bank in accordance with prudential and security regulations, as they may vary over time, cannot be met.

Also, in order to **conclude or execute a contract**, to make the process of analyzing its requests more efficient, by evaluating the eligibility in relation to the relevant regulations, as well as to evaluate and monitor the possibility of repayment of the contracted debts, the Bank may carry out data processing and issues automated decisions regarding the analysis of a request for granting credit or providing investment products. These decisions may also involve the creation of profiles that take into account, in accordance with the Bank's risk policy, among others, the financial status, creditworthiness, credit risk, degree of indebtedness, payment behavior, debt history or, in some cases, experience with the respective products. Thus, for example, the client's requests for credit will be rejected if his risk profile does not meet the minimum criteria considered by the Bank in accordance with its policies and the applicable prudential regulations. The relevant criteria and algorithms, as well as prudential regulations, may vary over time.

Creating profiles or classifying customers into various categories based on criteria such as age, geographical area, product owned, frequency of use of certain products and services, income, types of expenses, transaction data, etc. and, in relation to these profiles or categories, automated individual decisions may also be used to send personalized commercial communications based on **the consent** of the data subject expressed under the conditions specified above and/or **the legitimate interest** of the Bank.

Under the GDPR regulation, in all cases, the data subject has the right to obtain a reassessment of the decision on the basis of a human intervention, the right to express his / her point of view regarding the automated decision, as well as the right to challenge that decision.

Recording of phone calls and video monitoring

The Bank may record and keep any phone conversations as well as any video recordings, made with the data subjects according to the legal provisions and/or its internal rules, in order to prove various operations, instructions or agreements expressed by or for the client or another data subject, including in the case of contracts concluded remotely, to prove the content of interactions, instructions, requests and/or complaints made by

phone or other remote communication means, as well as the Bank's response, to use them as evidence to demonstrate compliance with legal or contractual obligations of the Bank or in case of disputes, to investigate various situations or to improve the quality of its services.

The data subject will be informed about the recording of a phone conversation through pre-recorded messages or, as the case may be, through information provided by a human operator, the continuation of the call confirming the consent of the data subject for the recording of the call.

The refusal of the data subject to accept the recording of a telephone conversation may determine the impossibility of the Bank to offer certain products or services or to accept and execute certain instructions (such as those concluded even through the telephone as a means of remote communication). In the other cases, the refusal of the data subject to accept the registration will not affect the resolution of the requests or the complaints, but they will have to be sent to the Bank through the other communication channels made available (email, postal address), in which case the response time from the Bank may be longer.

In order to ensure a high level of security, in accordance with the legal requirements regarding the safety and security of the financial-banking activity, the Bank video monitors all the premises of the units in which it operates, as well as the area of its own ATMs. Video monitoring is indicated by appropriate signs, and the records are kept for the period provided by law or for a longer period at the request of the authorities or in case of a legitimate interest derived, for example, from ongoing investigations.

If you have requested a product or service for which there is also the possibility of identifying you through image processing, you will be notified separately.

➢ WITH WHOM DO WE SHARE THE DATA?

In order to carry out the activity and ensure the provision / offering of banking services to the client, safely, at the best standards or in order to fulfill its legal obligations or in pursuit of its legitimate interests as detailed in this policy, the Bank may disclose personal data to certain persons or entities, in particular to:

a) the data subject himself (for example for data deduced by the Bank or received from third parties), legal representatives (for example: guardian, curator), the powers-of-attorney of the data subject or the client;
b) third parties such as the corresponding financial institutions, clearing / settlement entities or entities involved in the execution or facilitation of the fund transfer services (such as: SWIFT, STFD Transfond SA, ReGIS, SENT, card issuers - VISA, Mastercard, the merchant banks to which the customer made the card payment, payment institutions of the beneficiaries of the funds transfers from

the Bank's client accounts), including for the purpose of clarifying possible operational errors or potential fraud, as well as entities guaranteeing loans/deposits or various types of loans (applicable guarantee schemes, such as the Deposit Guarantee Scheme of the Kingdom of the Netherlands, credit guarantee funds under various government programs, etc.), entities that ensure the necessary infrastructure for: the operation of online payment services (3D secure), the issuance and use of virtual cards or the use of virtual POS, the issuance and use of advanced or qualified electronic signatures, the use of cloud services, the operation of the Beneficiary Name Display Service (SANB);

c) insurance - reinsurance institutions of the Bank's risks;
d) insurance - reinsurance institutions of the client's risks, when, for example, the client benefits from an insurance policy, whether or not it is related to a product offered by the Bank or requires the facilitation of its conclusion;
e) the persons who guarantee a client obligation assumed towards the Bank;
f) any of the persons / entities belonging to the group to which the Bank belongs, including any entities from the Fiba group or Nexent Bank where, for example, the technical processing or business strategy at group level of the data is located, analyzed, decided and / or centralized;
g) the majority shareholder of the Bank and other entities in its group, in particular for the purposes of organizing supervision on a consolidated basis and for combating money laundering and terrorism financing, as well as for ensuring uniformity and implementation of internal strategies and standards at group level and / or of group-level recommendations from authorities, auditors, consultants;
h) any of the consultants of the Bank and / or of the entities belonging to the group of which the Bank is a part or even to the data subject (for example, in legal, fiscal / financial, economic, technical matters), as well as judicial administrators, liquidators, bailiffs, auditors, lawyers, mediators, arbitrators, notaries, evaluators, experts, translators;
i) any other third party/entity, to the extent that disclosure is necessary to initiate a relationship with the Bank or to provide services contracted by the client from the Bank or that person/entity is directly or indirectly involved in providing services to the Bank, such as in the case of entities such as third-party payment service providers or in the case of services outsourced or contracted by the Bank from specialized providers or in order to secure operations and optimize the business, such as: remote identification services, identity and identification data verification services including by reporting to databases managed by public or private entities, services related to the granting, use and validation of electronic signatures, statement and notification printing services, courier services, message transmission, debt collection, hosting and administration of web services, software maintenance and development services, IT services, card providers and services for using cards or other payment instruments with remote

access, data security service providers and/or transactions, archiving services, document destruction services, debt collection agencies, ATM/POS maintenance service providers, real estate agencies, notary, legal services or other types of consultancy, assistance or representation;

j) professional associations, such as the Romanian Association of Banks and local financial and banking supervisory authorities or of the mother bank in the Netherlands (for example, National Bank of Romania, Central Bank of the Netherlands, the Financial Supervisory Authority, etc.), competent authorities at the local or European level in tax matters, consumer protection authorities, competition supervision, personal data processing supervision, competent authorities in connection with the merger operations in which the Bank is involved (for example, the National Registry Office Commerce);
k) credit agencies, mainly for assessing the Bank's credit risk;
l) any entities within the Bank's group (such as Nexent Bank N.V. based in the Netherlands) or outside it, with which the Bank is in negotiations or for carrying out due diligence by the respective entities, in view of or in the context of a transaction with these entities for the disposal/transfer or acquisition of assets, merger, acquisition, transfer, sale/purchase of contract portfolios, receivables or business parts, or other similar transactions regarding the Bank's rights and/or contracts in relation with the client/data subject, including the consultants of these entities, as well as later for the implementation/execution of the respective transaction, with the application by the Bank of appropriate measures to guarantee the rights of clients/data subjects in the context of these operations;
m) entities such as the Credit Bureau, the Central Credit Register, the Payment Incident Register, any other entities / institutions (for example: credit, leasing, insurance and utility companies),
n) courts, alternative dispute resolution centers, arbitration courts and other authorities or entities authorized by law to request and receive information from credit institutions (for example, enforcement bodies, structures established in the form of the Central Banking Risks, the Central Payment Incidents or the Deposit Guarantee Fund);
o) The National Agency for Fiscal Administration, for the purpose of transmitting information, in accordance with the law, to the tax authorities in the United States of America or Europe, in accordance with FATCA and CRS rules, as well as / or other entities with similar role.
p) public or private entities that manage databases of public sector bodies or private databases containing information from public authorities, such as, without limitation, the General Directorate for Personal Records, the Trade Register Office, the National Register of Personal Property, the Cadastre and Real Estate Advertising Office, the National Notarial Register of Powers of Attorney, etc.

➢ HOW LONG DO WE KEEP THE DATA?

The Bank will process personal data during the performance of banking services and the achievement of the respective data processing purposes, as well as subsequently in order to comply with the applicable legal obligations, including the provisions regarding archiving. In accordance with the applicable legal provisions, there are different archiving terms, depending on the type of data.

For example, according to the regulations, the data regarding the transactions must be kept up to 10 years after the end of the relationship with the client. The databases administered for the purpose of direct marketing will be processed for the duration of the consent of the of the data subject to receive such communications, as well as for a period considered necessary by the Bank to demonstrate compliance with the legal requirements (for example, 3 years from the withdrawal of the agreement). The data may be stored for a longer period of time at the request of the authorities or for the protection of legitimate interests (such as disputes or ongoing investigations).

➢ IMPLICATIONS OF REFUSING TO PROVIDE DATA

You may choose not to provide data to Nexent Bank, but this option may in some cases result in a non-compliance with our contractual or legal obligations and, as a result, may prevent us from continuing to provide or renew your existing products and services. In other cases, it may limit the services we are able to offer you or the promptness or flexibility of communication with the Bank.

If you do not agree with the processing of the data for marketing purposes, as well as in the event that you withdraw your previously expressed consent to processing for marketing purpose, your contractual relationship with the Bank will not suffer.

➢ PROCESSING DATA OUTSIDE THE EUROPEAN ECONOMIC AREA (EEA)

Currently, in order to fulfill the above-mentioned purposes, it is possible for the Bank to transfer certain categories of personal data outside Romania, to EU/EEA countries that provide an adequate level of data protection: the Netherlands (where Nexent Bank N.V. is registered and authorized as a credit institution), Malta (where group entities are located or as a beneficiary of information technology services), or outside the EU/EEA, to Switzerland (in the case of using SWIFT), the United States of America (in the case of using SWIFT and, potentially, FATCA reporting), Turkey (in the context where group entities are located or as a beneficiary of information technology services) as well as for CRS reporting. For transfers outside the EU/EEA, the Bank will base its transfer of personal data either on adequate data protection safeguards, such as standard

contractual clauses adopted at the European Commission level or other safeguards recognized by law, or on the fulfillment of other conditions according to applicable regulations. For example, the Bank will transfer personal data abroad when this transfer is necessary for the execution of a contract it has concluded with the client/data subject, for example when executing instructions to transfer funds from the client to third countries.

It is possible that during the course of the activity the transfer states mentioned above will change. Through this policy, which we will review periodically, we will ensure the updated information of clients and other data subjects regarding the list of states where personal data is transferred.

FATCA (The Foreign Account Tax Compliance Act). CRS (Common Reporting Standard)

FATCA is a set of legislative measures issued by the Treasury of the United States of America (IRS) that aims to prevent and reduce tax evasion generated by the activity of American citizens and residents who hold accounts outside the US territory. FATCA imposes on non-US financial institutions the obligations to:

(a) specific identification and monitoring of their clients' data for FATCA purposes,

(b) reporting of clients falling under FATCA,

(c) retention of a penalty fee, if applicable.

CRS is a mandatory reporting standard issued by the Organization for Economic Cooperation and Development (OECD), the Council of the European Union adopting in this sense Directive 2011/16/EU on administrative cooperation in the tax field and which establishes the framework for the automatic exchange of financial information on residents member states of the European Union. The CRS imposes on the financial institutions the obligations of

(a) specific identification and monitoring of residence data and fiscal identification,

(b) reporting of clients who fall under the CRS incident.

The bank carries out its activity in compliance with FATCA and CRS requirements. In this sense, the Client expressly undertakes:

(a) to communicate to the Bank, immediately and in writing, any change in his identification data provided to the Bank at the initiation or during the business relationship with the Bank, submitting the relevant documents to the Bank, so that the Bank can monitor and categorize the client for FATCA/CRS purposes,

(b) to immediately provide the Bank, at its request, with any information and documents that the Bank considers relevant for FATCA/CRS purposes.

The client understands and agrees that, in case it is or becomes subject to FATCA/CRS requirements and in order to fulfill its obligations under FATCA/CRS, the Bank: (a) may transmit the client's information and documents to the competent tax authorities (from Romania or abroad), (b) may withhold from the client's accounts opened at the Bank the amounts having a US source, in accordance with FATCA requirements, which we will transfer to the competent tax authority (from Romania or abroad), the Bank being exempted from any responsibility in these cases.

➢ WHAT CAN YOU DO TO HELP US KEEP YOUR DATA SECURE

We make constant efforts to maintain data security. However, your vigilance also helps us. We recommend setting strong passwords and please do not disclose them to anyone. Do not leave the devices connecting to the banking applications unattended and keep in mind that any communication to the Bank, via email or other similar channels, is not under the control of the Bank. Report to bank any suspicious activity regarding your accounts immediately. For details regarding data security, please visit the Data security section.

➢ RIGHTS OF THE DATA SUBJECTS

In the context of the processing of personal data, both the client and the other data subjects benefit of certain rights in relation to the Bank that can be exercised upon request and free of charge, and to the extent that the legal conditions are met, as follows:

The right to be informed – the right to be informed about the identity and contact details of the Bank and of the data protection officer, the purposes of the processing, the categories of processed data, the recipients of the data, the existence of the rights provided by the applicable law and the conditions under which they can be exercised;

The right of access to data - the right to obtain confirmation that personal data are or not processed by the Bank;

The right to rectification – the right to request and obtain the correction of inaccurate data, as well as the completion of incomplete data;

The right to erasure („the right to be forgotten") – the right to obtain the erasure of personal data;

The right to restrict processing – the right to obtain the marking of stored personal data, in order to limit their further processing;

The right to data portability – the right to receive personal data in a structured way, commonly used and in an easy-to-read format, as well as the right to have such data transmitted by the Bank to another data controller;

The right to opposition - the right to object at any time, for reasons related to the particular situation, to personal data processing based on public or legitimate interest, including processing for direct marketing purposes or by creating profiles;

The right not to be subject to an individual decision – the right to request and obtain the withdrawal, cancellation or re-evaluation of any decision based exclusively on processing carried out by automatic means (including the creation of profiles) that produces legal effects or similarly affects, to a significant extent, the data subject;

The right to file a complaint with an authority or to refer to the justice – The client has the right to file a complaint with the National Authority for the Supervision of Personal Data Processing, respectively to refer to the justice for the defense of any right guaranteed by the applicable legislation in the field of personal data protection, which have been violated, to the extent in which the data subject considers it necessary.

➢ HOW TO CONTACT US. DATA PROTECTION OFFICER

For more details regarding the personal data processing activities carried out by the Bank or in the event that you wish to exercise any of your legal rights in relation to the processing of Data as a data subject, you can send us a written request, dated and holographically signed (by hand), sent in paper format to any of our territorial units whose addresses you can find on the Bank website (here) or by e-mail at office@nexentbank.ro .

You can also address to the data protection officer by e-mail at dpo@nexentbank.ro or by letter at: **Nexent Bank N.V. Amsterdam Sucursala București,** Timișoara Boulevard no. 26Z, Anchor Plaza Building, District 6, Bucharest.

To the extent that you have suggestions regarding this Privacy Policy, we encourage you to send them to us at the e-mail address: dpo@nexentbank.ro

➢ CHANGES TO THIS POLICY

We will periodically review and update this Privacy Policy whenever necessary. The updated policy will be made available to you on this web page, as well as in our branches and agencies. Our policy update may also be notified to you by SMS, at ATM, email or when you log in to our applications online.

The privacy policy represents a statement of the Bank and has a legal nature distinct from that of the documents in which it can be incorporated by reference, and may be amended separately.

The information regarding the processing of personal data detailed by the provisions of this Privacy Policy is supplemented at any time and exclusively in addition to other information made available by the Bank, including without limitation, through: the General Business Conditions, the cookie policy, the information notes regarding the processing of personal data provided in the context of various specific products and services offered by the Bank, for example, the information regarding the processing of data in the Credit Bureau system provided upon requesting a loan, the information related to services such as internet banking and mobile banking, in the context of mobile phone applications, at ATMs, at the Bank's locations, during telephone calls with and/or without a human operator, in the context of remote identity verification using electronic means, including video means, in the context of using an electronic signature, etc.

Any information of the type exemplified above will be complementary or additional and will not restrict the area of the data categories, the purposes, the recipients or the basis for the processing of personal data as they are detailed by the Privacy Policy, by the General Business Conditions and / or by any other document, regardless of its name or type (application, form, convention, contract, agreement, annex, commitment, terms and conditions, information, notification, summoning, etc.) applicable in the relation between the Bank and the Client / the user or additional beneficiary regarding specific products and / or services provided by the Bank.