

NOTICE ON THE PROCESSING OF PERSONAL DATA OF CREDIABANK S.A.

CrediaBank S.A., which is based in Chalandri, at 260-262 Kifissias Avenue (phone no. 210 3669000) (hereinafter referred to as the "Bank"), in its capacity as Data Controller, provides you with the following information on the processing of your personal data in the context of your transactional relationship with the Bank, in accordance with Regulation (EU) 2016/679 (hereinafter referred to as "GDPR"), Law 4624/2019 and the relevant provisions of the Greek and EU legislation on the protection of personal data.

In particular, this notice concerns natural persons / data subjects who, in any capacity, have a transactional relationship with the Bank, such as, but not limited to, active, prospective and former customers, temporary customers, persons who have provided a guarantee or security in favor of the above persons, traders in general, suppliers and partners of the Bank, bondholders, creditors, beneficial owners of legal persons or entities, third parties related to the above persons (including but not limited to: proxies, agents, representatives, their employees/partners, shareholders, counterparties/customers' traders, where required to provide services e.g. payers or payees in payment service transactions, family members, lawyers, counterparties, procedural representatives, etc.).

This notice may be supplemented with more specific updates on a case-by-case basis (including but not limited to: cases of processing special categories of data, cookies, images from the Bank's video surveillance systems, etc.).

1. Which personal data are collected by the Bank and from where?

The Bank collects and processes the personal data necessary to achieve the intended purpose of processing. Personal data are collected either directly from you, either in the context of your contractual relationship with the Bank or from public authorities, bodies and third companies and always in a fair and lawful manner, as specifically mentioned below:

- 1.1. Your identification data**, such as your full name, father's name, mother's name, Identity Card or Passport details, TIN, Social Security number, gender, date and place of birth, nationality, signature data.
- 1.2. Your contact data**, such as your home address, mailing address, email address, landline and mobile phone number, as obtained from utility bills and fixed line and mobile phone bills.

The data under 1.1 and 1.2 are verified/updated directly by you or the Bank and directly collected from you or the Bank, where this is allowed, through databases, with or without your instruction/authorization (e.g. eGov-KYC of the General Secretariat for Information Systems), or through publicly accessible sources, such as, but not limited to, mortgage offices, land registries, courts, registers, etc, and/or from collaborators of the Bank debtor

notification companies (Law 3758/2009 as in force), credit and loan servicing firms (Law 4354/2015 as in force following the publication of Law 5072/2023), or lawyers and law firms, bailiffs and natural or legal persons in general, who undertake on behalf of the Bank to update your contact details in case you have failed to notify the Bank of any relevant change.

1.3. Data related to financial position, assets and family status such as professional details and work address, remuneration, tax forms E1, E9, the unified property ownership tax (ENFIA) and tax assessments, copies of payslips, insurance and/or tax certificates, documents of acquisition or transfer of movable or immovable property, tax residence, marital or non- marital status, dependents, etc.

Such data are verified/updated directly by you, persons authorized by you, or the Bank and directly collected from you, persons authorized by you, or the Bank, where this is allowed, through databases, with or without your instruction/authorization (e.g. eGov-KYC of the General Secretariat for Information Systems, e-EFKA of the National Social Security Entity, etc.), or through publicly accessible sources as such, including, but not limited to, mortgage offices, land registries, courts, tax authorities or data archives of TIRESIAS S.A. (see below).

1.4. Data on your financial defaults, such as bounced cheques, terminations of loan and credit agreements, orders for payment, seizures and calls for payment, applications and decisions to enter into pre-bankruptcy, bankruptcy or reorganization proceedings.

1.5. Data relating to your creditworthiness, such as your debts to credit and/or financial institutions from loans and credits, letters of guarantee and/or letters of credit, etc.

1.6. Data concerning your credit scoring – credit profiling.

1.7. Data of your transactional behavior, such as data resulting from the operation of your contract(s) with the Bank, in which you participate as a counterparty or in any other capacity, data from the use of the Bank's products and services as well as from documents and supporting documents that you submit or send to the Bank, as well as from questionnaires that you complete either during your contractual relationship or at a pre- contractual stage.

The data under 1.4.-1.7. are generated by and collected from the Bank's information systems in the context of your transactional relations with the Bank and/or from other credit and/or financial institutions, where allowed, and/or from financial behavior data files, mainly from the TIRESIAS S.A. systems (see below), as well as from debtor notification companies cooperating with the Bank (Law 3758/2009 as in force), credit and loan servicing firms (Law 4354/2015 as in force) or lawyers and law firms, for relevant cases assigned to them by the Bank.

1.8. Data on the execution of payment transactions and the provision of payment services, such as, but not limited to, data on the execution of transfer orders from/to a payment accounts, remittances, direct debit orders, transactions using

payment instruments, etc. These data are collected either from you or from payment service providers at your request. These data may include, in addition to your own data, data of third parties who are related to the payment transaction in their capacity of payer or payee.

- 1.9. Data from acquiring contracts** which have been terminated by the credit institutions or card issuing and management companies cooperating with you, for reasons that constitute a breach of the specific terms of the relevant contracts (e.g. acceptance of cards that have been declared as lost, virtual transactions, self-financing, etc.). These data are collected from the Bank and/or TIRESIAS S.A. (see below).
- 1.10. Investment profile and transaction data** including data about your knowledge and experience in the investment sector, your financial situation, your level of risk tolerance, your investment objectives, as well as data resulting from your investment transactions and/or the acquisition of investment products. In addition, this category includes data on the funds and financial instruments held by you and acquired through the Bank or held by the Bank in accordance with the applicable legislation. These data are collected directly from you and/or from the Bank in the context of your investment transactions with the Bank.
- 1.11. Data on transactions in financial instruments and the exchange or provision of financial information**, collected in the context of compliance with applicable legal or regulatory provisions (such as Regulation (EU) 648/2012 (EMIR), Regulation (EU) 600/2014 (MIFIR), FATCA, CRS, reportable cross-border arrangements (DAC6), etc.) and Greece's relevant international obligations.
- 1.12. Data related to the provision of insurance products** through the Bank's intermediary, such as data required for the conclusion of the insurance contract and the risks covered, as well as by the legal and regulatory framework. These data are collected directly from you.
- 1.13. Data resulting from guarantees/collateral** (including insurance) in the name or in favor of the Bank.
- 1.14. Data for assessing the risk of money laundering and/or terrorism financing**, which are collected directly from you, from your transactions, from TIRESIAS S.A. (see below) and from authorities and bodies responsible for the prevention and suppression of the aforementioned offences.
- 1.15. Data of beneficial owners of legal persons or entities** that are active, prospective or former customers of the Bank or traders in general.
- 1.16. Data identifying your electronic identity** and your connection to electronic banking services (e.g. e-banking, mobile banking), transactional behavior data relating to the general provision of electronic banking services and the use of electronic and/or digital products, services and applications of the Bank, such as Internet Protocol addresses (IP Addresses) or other online identifiers, such as location data, web browsing data (cookies) which –alone or combined with unique identifiers– may be used to identify you.

These data are collected directly from you, from the Bank's systems or applications

that you use, as well as from service providers cooperating with the Bank (e.g. Google).

- 1.17. Data of your telephone communications or video calls** with the Bank, recorded upon your prior notification, in accordance with the applicable legislation.
- 1.18. Image data from the video surveillance systems of the Bank's premises**, where the relevant legal signs exist (e.g. entrances of the Bank's branches and main buildings, transaction counters, ATMs).
- 1.19. Special categories of data**, such as your health data and/or that of your dependent family members, submitted to the Bank by you, in special cases (e.g. for the settlement of any debts) only on your own initiative, if you rely on them, as well as biometric data relating to the characteristics of your electronic signature and your facial image in the form of a dynamic-selfie, which you submit in the context of the remote identification procedure for the provision of products and services. These data are collected and processed by the Bank only if the legal requirements are met.
- 1.20. Data for the conduct of and your participation in draws, competitions and loyalty programs** of the Bank, which we collect from you or in the context of the operation of your contract(s) with the Bank or the execution of transactions as well as in the context of the use of the Bank's products or services.
- 1.21. Your qualified certificate for electronic signature** which is issued by the qualified trust service providers who cooperate with the Bank, and collected, in accordance with the applicable institutional framework.
- 1.22. Data of minors** (persons who have not reached the age of 18), which the Bank collects and processes subject to the prior consent of their parents or holders of parental responsibility, unless otherwise specified by the law.

Please note that:

- except for your data under (1.1) and (1.2), which are strictly necessary for your transaction or contractual relationship with the Bank, the type and amount of other data collected depends in each case on the type of a contract that will either be concluded or existing with the Bank and/or the product or service offered or supplied.
- You must previously inform properly any third parties (for instance, by reference to this notice) and obtain their consent, where required, if you wish to provide the Bank with their personal data.

The company under the name "Bank Information Systems S.A." and the distinctive title "TIRESIAS S.A." is responsible for the processing of financial behavior data on behalf of the banking system of the country, with the main purpose of evaluating the credit risk assumed by credit institutions. The company is based at 2 Alamanas Street, 151 25 Maroussi, its telephone number is +30 210 3676700 and the address of the website is www.teiresias.gr. Access to the records of "TIRESIAS S.A." is possible without your prior consent, if it is deemed necessary for the establishment or maintenance of your transactional relations with the Bank.

You may be informed by TIRESIAS S.A. about the processing of your data as well as the

exercise of your rights at the above telephone number and/or the above site.

The Bank may collect data of the same categories as those held by TEIRESIAS S.A. from other company records that operate legally in Greece or in another Member State of the European Union.

2. Why do we collect your personal data and what legal basis do we use to process it?

The Bank collects and processes your personal data as appropriate each time it is necessary based on the following legal grounds / legal basis for processing and the respective purposes, as detailed below:

2.1. For the performance of a contract or the evaluation of your request before the conclusion of the contract

The personal data referred to under 1 are processed for the following purposes:

- 2.1.1.** for the identification and verification of your data;
- 2.1.2.** for the communication with you at the stage of both the pre-contractual and contractual relationship with you, as well as for issues relating to any other transaction or cooperation with the Bank, such as, but not limited to, informing you on how to make better use of the products or services that the Bank provides you (e.g. the possibilities, opportunities for use, new functionalities and their developments), informing you about participation in the Banks's loyalty programs, draws and competitions and the possible selection of you as a winner;
- 2.1.3.** for the assessment of your general requests, conclusion and proper performance of contracts with you, fulfillment of the Bank's obligations towards you, as well as handling, support and monitoring of your transactions;
- 2.1.4.** in the case of granting any loan or credit, the data are processed for:
 - the credit risk assessment that the Bank is called upon to undertake or has already undertaken;
 - the tracking of the progress of the debt;
 - preventing or limiting the likelihood of any breach of your obligations on your part under your contract(s) with the Bank; and
 - seeking any amounts owed to the Bank from the operation of your contract(s) with it;
- 2.1.5.** the handling, support and monitoring of all forms of transactions through electronic banking, such as e-banking, mobile banking and the Your Attica telephone service;
- 2.1.6.** the assessment of your suitability and compatibility for the provision of investment products and services or services in the insurance sector, your update about them, monitoring those products and your inclusion, if possible, in the identified target market for these products;
- 2.1.7.** the management of portfolios of loans and credits outsourced to credit and loan servicing firms, in accordance with the applicable legislation on their operating

framework and for the outsourcing of credit institution loans servicing to them;

- 2.1.8.** the representation of the debenture holders pursuant to Article 4 of Law 3156/2003 as in force;
- 2.1.9.** your update (debtors and/or guarantors) on the debts owed before or after the termination and/or performance of the necessary preparatory actions for the extrajudicial and judicial pursuit of the collection by the Bank of the overdue and receivable debts in accordance with the provisions of Law 3758/2009, as in force.

The above purposes of data processing are also applicable and must be attained for: the fulfillment of the Bank's legal obligations (mentioned below in Section 2.2.) as well as for serving the legitimate interests of the Bank or a third party (below in Section 2.3.).

2.2. for the Bank's compliance with its legal obligations

In particular:

- 2.2.1.** for the general compliance of the Bank with its obligations imposed by the applicable legal and regulatory framework (including the applicable state aid and tax legislation, as well as the provisions concerning the automatic exchange of information in the field of taxation) and the decisions of supervisory or judicial authorities;
- 2.2.2.** for preventing and tackling money laundering and terrorism financing;
- 2.2.3.** for the security of transactions and the protection of the property, safety and physical integrity of employees and customers or visitors of the Bank;
- 2.2.4.** for the assessment of your creditworthiness, where applicable and necessary for the maintenance of your transactional relationship. Please note that, in order to fulfill this purpose, we may adopt partially automated decision-making, including credit profiling (see Section 2.5 below);
- 2.2.5.** for the assessment of the compatibility and any other assessment or categorization of the customer, as appropriate, for the creation or provision of a financial instrument or service;
- 2.2.6.** for the execution of payment transactions initiated by you or at your request, such as, but not limited to, the recording and archiving of all orders given by customers for the execution of transactions in financial instruments, including the obligation to record orders given by telephone;
- 2.2.7.** for the Bank's compliance with obligations arising from its contracts with co-financing or guarantee institutions/organizations or third parties in general;
- 2.2.8.** for any relevant notification and transmission to the competent Supervisory, Independent, Police, Judicial and Public Authorities in general, as well as to third legally authorized legal entities, where required in accordance with applicable legislation;
- 2.2.9.** for your identification by the Bank, as a Registration Authority, in the context of a request submitted to a qualified trust service provider for the issuance of a qualified digital certificate, in accordance with Regulation (EU) 910/2014 (eIDAS);
- 2.2.10.** for your telephone service through the call center. Please note that to the extent that your communication with the telephone center involves handling of your transactions the relevant calls will be recorded for proof/verification and transaction security purposes.

The above purposes of data processing are also applicable and must be attained: for the

fulfillment of the legitimate interests of the Bank or a third party (see Section 2.3 below).

2.3. for the purpose of protecting the rights and legitimate interests of the Bank or a third party

In particular:

- 2.3.1.** for the investigation of your level of satisfaction with the Bank's support and services provided and/or your further wishes or requirements, in order for us to develop and improve the efficiency of the Bank's products and/or services, as well as to design and offer new or similar products to those you have already received, in accordance with the relevant applicable legal and regulatory framework;
- 2.3.2.** for managing your complaints or resolving any requests you may have;
- 2.3.3.** for the security of the Bank's IT systems, facilities and assets, the prevention of criminal activity or fraud against the Bank or third parties from any external risk or threat;
- 2.3.4.** for the transfer, assignment and/or securitization of part or all of the Bank's claims from credits and loans, as well as the outsourcing of their management (servicing) to any third party(-ies), including the management by the Bank itself of loan claims purchased from another credit or financial institution or which it has undertaken to manage based on the relevant legal provisions (inter alia: Law 3156/2003, Law 4354/2015, Law 5072/2023), as in force;
- 2.3.5.** for the protection of the legitimate rights and interests of the Bank or companies of its Group against third parties and/or the assertion of its legitimate claims before judicial authorities or other administrative or independent public authorities and out-of-court/alternative dispute resolution bodies or co-financing entities, etc.

2.4. With your consent

In case the processing of your personal data is not based on any of the legal bases mentioned above under Sections 2.1. to 2.3., the Bank will process your personal data only if you have previously provided your explicit consent, for the purposes listed below:

- 2.4.1.** for your update on new products and/or services of the Bank, companies of its Group and/or its affiliated companies (via Viber, telephone, email, sms and other electronic means of communication);
- 2.4.2.** for automated decision making (see Section 2.5 below);
- 2.4.3.** for any transmission of your data to third countries outside the EEA where applicable (see Chapter 4);
- 2.4.4.** for understanding how you use and interact with the content of our website through the use of cookies;
- 2.4.5.** for the completion of the printed or electronic forms for the expression of interest in products, services or actions of the Bank or its cooperating companies;
- 2.4.6.** for the processing of your biometric data in the context of your remote electronic identification, where applicable.

In such cases, you have the right to withdraw your consent at any time without prejudice to the lawfulness of the processing based on your consent until its withdrawal. To find out how to withdraw your consent, please check the information in Chapter 6 below.

2.5. Profiling – Automated decision making

The Bank may make decisions based on mathematical methods and statistical analyses of those parameters that are deemed necessary for the purpose, through automated procedures involving your profiling in particular when: (i) it is necessary for the conclusion or performance of a contract with the Bank; (ii) it is permitted or required by the EU or national law; or (iii) you have given your explicit consent, in particular when the automated decision cannot be based on other legal grounds. In any such case, you have the right to object to the automated decision and to request a review, by human intervention, of your rejected request, as set out in Chapter 6 below.

In particular, the Bank may lawfully make such decisions, including profiling, by combining the processing of your personal data for the purposes of:

- 2.5.1.** Promotion of new products and services, unrelated or related to those you have already received from the Bank, companies of its Group or companies cooperating with the Bank, provided that you have previously given your explicit consent. The Bank may profile you using the combined data mentioned above and for the purpose of informing you, which does not constitute "promotion". The relevant processing in this case serves both the performance of your contract with the Bank and the legitimate interests of the Bank or a third party.
- 2.5.2.** For your classification as a retail or professional client, which is mandatory and in accordance with the Directive of the European Parliament 2014/65/EU (MiFID II) transposed into Greek law by Law 4514/2018 and its implementing measures, as applicable, etc. and for the assessment of your suitability and compatibility for the provision of investment services/products and your tolerance to investment risks as well as for the provision of services/products in the insurance sector. In this context, the Bank processes your personal data in compliance with its relevant legal obligations.
- 2.5.3.** For the risk assessment and for the mandatory adoption of measures for the prevention and suppression of money laundering and terrorism financing (Law 4557/2018, as in force). In this context and in compliance with the above legal obligation, the Bank, using international standards and recognized evaluation models, processes combined data such as identification data, data related to financial position and assets and data from the execution of payment transactions.
- 2.5.4.** For the assessment of your creditworthiness (credit scoring) which is based on personal data, obtained directly from you or from a search in the financial behavior database of TIRESIAS
S.A. and for which (assessment) the criteria taken into account are your (since you are the data subject) income, your financial obligations, your profession, your compliance with your contractual obligations under previous financing received

from the Bank or a third party creditor. The above processing is necessary for the conclusion and operation of a loan agreement but also in order to limit the credit risk assumed by the Bank, limit bad debts and protect you from over-borrowing.

3. Who are the recipients of your personal data?

The recipients of your data are only the necessary, in each case, staff of the Bank, who are responsible for the evaluation and management of your requests for the provision of products and/or services, for the management and operation of the contract(s) you sign with the Bank, for the fulfillment of the obligations arising from the contract(s), as well as relevant obligations imposed by law. In addition, recipients of your data are:

3.1. Businesses (sole proprietorships /natural persons or legal persons) to which the Bank outsources the performance of specific tasks on its behalf, subject to the condition of professional secrecy and the duty of confidentiality and discretion, such as, but not limited to:

- debtor/guarantor notification companies concerning your debts before or after the termination and/or performance of the necessary preparatory actions for the extrajudicial and judicial pursuit of the collection by the Bank of the overdue and receivable debts in accordance with the provisions of Law 3758/2009, as in force;
- companies to which claims of the Bank are transferred, such as vehicle corporations in the context of securitization and management (servicing) of credit and loan claims (purchasers or credit servicers under Law 5072/2023, as in force, subject to the provisions of Law 3156/2003) or companies to which the management of the Bank's claims (credit/loan servicing) has been entrusted or Credit and Loan Purchasing Firms in accordance with the applicable legal framework;
- call centers;
- data processing companies for the purposes of identifying you and verifying and confirming the authenticity of your data and updating them through a secure interface with the information system of the Public Administration's single digital portal in accordance with the applicable legislation;
- risk management service providers;
- companies active in digitization, storage, archiving, management and destruction of files and data;
- market analysis and research companies and customer satisfaction companies, advertising companies and companies for the promotion of products;
- companies providing specialized payment services;
- invoice issuing and sending companies;
- lawyers, law firms, notaries, bailiffs, experts, specialists, engineers and property valuers;
- chartered accountants/auditors and providers of advisory (e.g. technical, organizational, IT, financial, etc.) services, within the scope of their competences;
- mediators under Law 4640/2019 and mediation centers (e.g. Organization for Mediation and Arbitration – OMED);

- postal service providers;
- custody and physical security companies;
- providers of services for the supply, development, maintenance and configuration of IT applications;
- providers of remote electronic customer identification and verification and authentication of documents that you submit at the start of the remote transaction relationship with the Bank, providers of e-mail services, providers of internet hosting services including cloud services and cybersecurity service providers;
- depositary service providers;
- businesses that participate in the Bank's customer loyalty or reward programs to provide you with benefits from these programs.

3.2. In case of inclusion in pre-bankruptcy, bankruptcy or reorganization proceedings or debt settlement in general (under, *inter alia*, Law 3869/2010, Law 4469/2015, Law 4605/2019, as applicable), the Bank sends to the other involved credit or financial institutions and other companies of the Bank's Group, which may hold claims against the applicant, data on the applicant's / customer's loans and deposits and if it holds a claim against the applicant for any reason, it receives the corresponding data from the above institutions and companies.

3.3. Entities in the broader financial sector, including domestic or foreign investment companies, in the event of assignment of claims arising from loan agreements.

3.4. Credit institutions and/or financial institutions (based in Greece or abroad, that have obtained the required operating license and operate legally), international and domestic payment and digital transaction service providers, electronic money institutions for the performance of a contract with you or transactions you have requested or carried out, such as SWIFT, SEPA, VISA, MASTERCARD, etc..

3.5. Companies in the Group's financial sector, in order to estimate the total risk assumed, to

meet the supervisory obligations and to treat the Group's customers in a unified manner.

3.6. Supervisory, Judicial, Independent and other Authorities at national and European level for the fulfillment of the Bank's obligations under laws or regulatory provisions or court decisions, such as, but not limited to: the Bank of Greece, the European Central Bank, the European Competition Commission, the Hellenic Capital Market Commission, the Hellenic Competition Commission, the U.S. Securities & Exchange Commission (SEC), the Financial and Economic Crime Unit (ΣΔΟΕ), the Hellenic Financial Police, the General Secretariat of Commerce and Consumer Protection, the Hellenic Financial Ombudsman, the Public Authorities in Greece and abroad, Courts, Public Prosecutors, Investigating Officers, etc. within the scope of their responsibilities.

3.7. "Interbanking Systems S.A." ("DIAS S.A.") for interbank transactions.

3.8. TIRESIAS S.A. for data relating to the records held by it and specific data relating to unsecured cheques, unpaid bills of exchange, unpaid bills of lading, termination of loan or credit agreements, loan and credit agreements and their development,

as well as contracts for the provision of guarantees, etc., for the purposes of the aforementioned objective, as well as for the purposes of public interest, which are ensured by the use of the Tiresias Risk Control System (TSEK), as detailed on the website of the aforementioned company (www.teiresias.gr).

3.9. Co-financing or guarantee institutions, where applicable, such as, but not limited to, the Hellenic Development Bank (EAT), the Deposit and Investment Guarantee Fund (TEKE), the Greek State, the European Investment Fund (EIF), the European Investment Bank (EIB), the Recovery and Resilience Fund, the Export Credit Insurance Organization (ECIO), etc. The recipients of the data sent to bodies such as the above-mentioned may also be any Greek or European Authority involved in the action and in the management of the respective body, in accordance with the specific provisions of the legislative and regulatory framework governing the action in question.

3.10. Investment firms (AEPEY), mutual fund management companies (AEDAK), other financial organizations or institutions or other authorities in the context of supporting your transactional relationships concerning the provision of investment services (e.g. Central Securities Depository, Stock Exchanges, Capital Market Commission, execution and trading venues, clearing and settlement systems and companies, trade repositories).

3.11. Insurance funds, public organizations, chambers of commerce and public enterprises.

3.12. Insurance companies and insurance intermediaries for the provision of insurance products.

3.13. Real estate management or real estate investment companies.

3.14. Qualified trust service providers in accordance with Regulation (EU) 910/2014 (eIDAS), as currently in force in the context of issuing a qualified certificate for electronic signature.

3.15. Virtual data room (VDR) providers to support and facilitate the management/access to loan portfolios for the fulfillment of the legitimate processing purposes, in compliance with the applicable law.

3.16. Any third persons who submit a request to the Bank for information in accordance with the legal requirements, such as account/asset managers or administrators of wills, etc..

3.17. Potential or existing purchasers of all or part of the Bank's activities or assets (including rights) and/or those entitled to encumber assets (including rights) of the Bank.

Please note that, in the event that the Bank outsources the processing of personal data to third parties, who either act on its behalf or as independent controllers, it first ensures compliance through specific provisions in the relevant contractual texts and the application of appropriate measures for the protection of such personal data.

4. Are your data transmitted to countries outside the European Economic Area (EEA) or to an international organization?

In the context of implementing the relevant operations and in compliance with the provisions of the applicable regulatory framework, the Bank may transmit your personal data to countries outside the European Economic Area (EEA) - (third countries) provided that an adequate level of protection of personal data is ensured by the third country on the basis of a decision of the European Commission or where appropriate safeguards have been adduced for the processing of your personal data, including binding corporate rules, in accordance with the law. If none of the above conditions apply, your personal data may be transmitted to the third country only if the conditions expressly provided for in European and national legislation are met (such as in the case where the transmission is governed by an international or transnational agreement, for reasons of public interest, or where the transmission is necessary for the performance of a contract or the execution of your order or if you have given your consent, etc.).

Please note that the Bank, through competent national authorities, may transmit your personal data in the context of implementing the legislation for the common reporting standard developed by the Organization for Economic Cooperation and Development (OECD), or in the context of the FATCA (Foreign Account Tax Compliance Act).

5. How long do we keep your personal data?

Your personal data are kept for as long as it is necessary for the fulfillment of the purpose of their processing, otherwise for the time required by the applicable legislation and in any case for a period of not more than (20) twenty years from the date of any termination or expiry of your contract or transaction, which is the time corresponding to the general limitation period for claims.

In particular and for instance:

- 5.1.** Your personal data relating to the conclusion and operation of the contract, including the supporting documents as well as those produced during the term of the contract, are kept at least throughout the duration of the relationship between the Bank and you, until the full repayment of each relevant debt/claim and the completion of the twenty-year period from the above repayment.
- 5.2.** If until the end of the twenty (20) years there are ongoing legal proceedings with the Bank or any affiliated company with it, which directly or indirectly concern you, this retention period of your personal data will be extended until an irrevocable court order is issued.

- 5.3. In the absence of a contract with the Bank, your personal data will be kept for five (5) years from the rejection of the application.
- 5.4. In the event that the law or regulatory acts provide for the retention period of your personal data to be shorter or longer, the above data retention time will decrease or increase accordingly.
- 5.5. Documents bearing your signature and to which your personal data has been registered may, at the sole discretion of the Bank, be kept electronically / digitally after five (5) years.

After the expiry of the above time periods, the Bank will delete your personal data in accordance with the framework and principles it applies for the maintenance and destruction of records and data.

6. What rights do you have to protect your personal data?

As a data subject you have the following rights:

- 6.1. To know what personal data we keep and process, their origin, purposes of their processing, the data recipients, and the time they are retained (**right of access**).
- 6.2. To request the correction and / or completion of your personal data so that it is complete and accurate (**right of rectification**). In these cases, you must provide any necessary documents that may indicate the need for such correction or completion.
- 6.3. To request the limitation of your data processing where certain conditions are met (**right of restriction**).
- 6.4. To refuse and / or oppose any further processing of your personal data we retain (**right of appeal**).
- 6.5. To request the deletion of your personal data from the files we hold, where certain conditions are met (**right to erasure**).
- 6.6. To request the transfer of your personal data to any other processor of your choice, under the applicable terms and conditions (**right to data portability**).
- 6.7. To request not to be subjected, where applicable, to a **decision-making** process **based solely on automated processing**, including profiling, which produces legal effects concerning you or significantly affects you in a similar way.
- 6.8. To withdraw at any time your consent in those cases where such consent is a legal basis for the processing of your personal data.

Please note the following in relation to your above mentioned rights:

- The satisfaction of your rights under (6.3), (6.4) and (6.5) insofar as it relates to data necessary for the preparation and / or continuation of the operation of the contract (s), irrespective of the source of their collection, results in the automatic termination thereof.

- The Bank may in any case have the right to refuse the satisfaction of your request to restrict the processing or deletion of your personal data if the processing or retention of the data is necessary for the establishment, exercise or support of its legal rights or the fulfillment of its obligations.
- The exercise of the right to portability (above, under 6.6) does not imply the deletion of your data from our records, which is subject to the terms of the immediately preceding paragraph.
- The exercise of these rights acts for the future and does not concern data processing already carried out.

7. How can you exercise your rights?

For the exercise of these rights, as well as for any matter concerning your personal data, you may contact:

- the Bank's Data Protection Officer (DPO) either by e-mail at the following address dpo@crediabank.com or by physical mail to: CrediaBank S.A., 260-262 Kifissias Avenue, Postal Code 152 31, Chalandri;
- at any branch of our Bank's network by filling out the Exercise of Rights form;
- on the website of the Bank www.crediabank.com, by filling out the contact form.

In such cases we will make every effort to respond to your request within thirty (30) days of its submission. This period may be extended for up to sixty (60) additional days, if deemed necessary by the Bank's absolute discretion, taking into account the complexity of the request and the number of requests, so we will inform you accordingly within the aforementioned period of thirty (30) of days.

Exercising your rights does not entail any charge. If however, your requests are obviously unfounded, excessive or recurrent, we may either ask you to bear the relevant reasonable costs for which we will inform you or refuse to respond to them.

8. Right to lodge a complaint

If, after exercising your rights as described above, you consider that: a) your request has not been adequately and lawfully met or b) your right to protect your personal data is infringed by any processing carried out by us, you have the right to lodge a complaint with the Data Protection Authority (postal address: 1-3 Kifissias Street, Postal Code 115 23, Athens, Greece, <https://www.dpa.gr>).

9. How does the Bank protect your personal data?

The Bank is committed to comply with the Personal Data Protection Policy as in force from time to time and to apply clear and rigorous procedures for the protection of personal data. It also undertakes to adopt and implement appropriate technical and organizational

measures to ensure a level of protection commensurate with the risks involved in the processing, as well as to maintain the confidentiality, integrity, availability and resilience of its systems or those of any third parties involved in the processing. Partners, agents, employees or third parties are expressly authorized by the Bank for such processing and are bound by discretion and protection of classified information clauses or are subject to the corresponding regulatory obligation of confidentiality and secrecy.

The measures we take are reviewed and amended at regular intervals or when deemed appropriate based on new needs and technological developments.

10. Contact

details DATA

CONTROLLER

CrediaBank

ADDRESS: 260-262 Kifissias Avenue, Postal Code 152 31, Chalandri

TELEPHONE: +30 210 366 9000

DATA PROTECTION OFFICER

ADDRESS: 260-262 Kifissias Avenue, Postal Code 152 31, Chalandri

Email: dpo@crediabank.com

11. Update - Amendment of this Notice

This document replaces any previous notices on the processing of personal data that may have been included in contractual or other documents of the Bank.

The Bank may amend/complete/update this notice in accordance with the applicable regulatory and legislative framework. In this case, the updated notice will be posted on the Bank's website at www.crediabank.com/en/personal-data-protection-gdpr/ and will be available in hard copy at any branch of the Bank's network.