

PRIVACY NOTICE

Ancoria Bank Ltd (hereinafter the “Bank”), in full transparency and respect of your rights and personality, collects and further processes personal data only for specified, explicit, and legitimate purposes, within the scope of its business relationship with you.

This Privacy Notice (hereinafter the “Notice”) provides an overview of how the Bank processes personal data in accordance with the applicable legal and regulatory framework, and particularly with the General Data Protection Regulation, 2016/679, of the European Union (hereinafter the “GDPR”).

The Notice is addressed to the following categories of natural persons:

- Existing customers of the Bank;
- Other individuals (non-customers) who maintain a business relationship with the Bank, such as guarantors, guardians of minors, beneficial owners, directors, shareholders, authorised signatories or secretaries of legal persons;
- Customers or other individuals who used to have a business relationship with the Bank in the past;
- Prospective customers of the Bank.

1. Who we are

Legal Name: Ancoria Bank Ltd
 Registration No.: HE 324539
 Address: 12 Demostheni Severi Avenue, 1st Floor, 1080 Nicosia
 P.O. Box 23418, 1683 Nicosia, Cyprus
 Phone Number: +357 22 849001
 Fax Number: +357 22 849002
 Email: info@ancoriabank.com
 Website: www.ancoriabank.com

Contact details of the Data Protection Officer of the Bank:

Address: 12 Demostheni Severi Avenue, 1st Floor, 1080 Nicosia
 P.O. Box 23418, 1683 Nicosia, Cyprus
 Phone Number: +357 22 849001
 Fax Number: +357 22 849002
 Email: dpo@ancoriabank.com

2. What personal data is collected and from which sources?

Personal data refers to any information about you that establishes or can establish your identity, such as your name and surname, your residential address, your telephone number and/or your ID/Passport number.

The Bank processes personal data it receives from you in the course of its operation as an authorised credit institution, as well as personal data it lawfully receives from third parties (e.g. companies that process card payments such as JCC Payment Systems Ltd, EveryPay Payment Services S.A. and Marqeta Inc.). Additionally, the Bank may also collect and/or otherwise process personal data from databases and/or publicly accessible sources (e.g. the Land Registry Office, the Registrar of Companies and Official Receiver, the Bankruptcy Records, the Commercial Registry, the Media, gov.gr, LexisNexis, and the Internet).

For instance, when you apply for a credit facility, the Bank is legally obligated (see section 3.4 below) to perform the necessary credit and identity checks in order to verify the information you provided and assess your creditworthiness. This includes sharing your personal data with credit bureaus

(such as Artemis Bank Information Systems Ltd and/or Bank Information Systems “Tiresias” S.A.) in order to obtain information that concerns your credit history and creditworthiness. These checks contribute to responsible lending and substantially mitigate the risks associated with fraud, money laundering as well as any related illicit activities.

Indicatively, the personal data that the Bank may obtain and/or otherwise process is the following:

- **Personal information** (e.g. name, identity card/passport details, date, city and country of birth, contact details such as telephone number and email address, correspondence address, professional status, employment field, employer details, tax identification number, level of education, marital status, whether you hold or held a political office (politically exposed person - PEP);
- **Assets** (e.g. gross annual income, source of your wealth);
- **Authentication data** (e.g. specimen signature, biometric data);
- **Data related** to the Foreign Account Tax Compliance Act (FATCA) and the provisions of the agreement between Cyprus and the United States of America, information according to the provisions of the Multilateral Competent Authority Agreement on Automatic Exchange of Financial Account Information (CRS), and information according to the “Administrative Cooperation in the Field of Taxation Law (Law 205(I)/2012)”;
- **Other information/documents** (e.g. details regarding your business and financial profile, your creditworthiness such as data from credit reference agencies, property ownership, personal debts, insurance policy details, data arising from the execution of your instructions such as payment orders, details arising from contractual obligations between you and the Bank, recent audited financial statements or recent management accounts (for self-employed natural persons or natural persons the income of whom derives from legal persons controlled by them), copy of residence permit (for non EU-nationals));
- **Additional supporting documents**, where required (e.g. a copy of a payslip, tax return for the previous year, proof of address such as a utility bill) and other personal data related to the aforementioned categories.

3. Why is personal data required and what are the legal grounds for processing?

The purposes and legal grounds for processing your personal data vary according to your business relationship with the Bank, and are outlined below.

3.1 For the performance of a contract

The Bank processes your personal data in order to provide you with banking and financial services, in accordance to the contracts concluded with you and/or in the course of your application prior to the conclusion of a contract in order to complete your acceptance process as a potential customer for the specific product/service, and/or to execute your orders.

3.2 For the purposes of legitimate interests

Where necessary and without prejudice to your fundamental rights and freedoms in relation to the protection of your personal data, the Bank processes your personal data to safeguard the legitimate interests pursued by the Bank or third parties.

These legitimate interests seek mainly to maintain the smooth operation of the Bank, and the safety of its clients and employees.

Some indicative examples where such processing is or may be performed are set out below:

- (a) in the context of the operation and security of the IT infrastructure of the Bank;
- (b) in the context of preventing and clearing up offenses;
- (c) in the context of preparing court proceedings and/or asserting legal claims;
- (d) in the context of the Bank’s risk management;
- (e) in the context of implementing a closed circuit monitoring system (CCTV) inside and outside the Bank’s Banking Centres, and in the Head Office building. The implementation of the

said system is done for purposes of preventing and deterring fraud, for collecting evidence for criminal offences, and/or for proof of payment purposes, such as withdrawals and deposits;

- (f) for purposes of improving the services and products of the Bank;
- (g) in the context of recording telephone calls for investigation as well as quality control purposes;
- (h) in the context of a public opinion research and/or research of the market in general, in case you have not exercised the right to object (extensively explained below in section 7(f));
- (i) in the event of transfer or assignment or sale or charge or creation of another collateral on any rights, title or interest of the Bank arising from any of your contracts with the Bank.

3.3 Due to your consent

If you consent to the processing of your personal data for specific purposes, e.g. collection and storing of biometric data, direct marketing, the legal basis for the processing of your personal data is your explicit consent.

It should be noted that you can withdraw your consent at any time (this also applies to any consent you provided prior to the 25th of May 2018). The said revocation does not affect the legality of the data processed prior to the revocation.

3.4 Due to compliance with a legal obligation and/or for the performance of a task carried out in the public interest

The Bank is subject to various legal obligations through which personal data processing is required, such as the "Prevention and Suppression of Money Laundering Activities" Law (N. 188(I)/2007), the Income Tax Law (N. 118(I)/2002), the "Cooperation in the Field of Taxation" Law (N.205(I)/2012), the "Business of Credit Institutions" Law (N. 66(I)/1997), the "Deposit Guarantee and Resolution of Credit and Other Institutions Scheme" Law (N. 5(I)/2016), the "Provision and Use of Payment Services and Access to Payment Systems" Law (N. 31(I)/2018), and the banking and tax legislation of the Republic of Cyprus in general as amended from time to time.

Furthermore, the Bank, as an authorised credit institution, is obligated to abide by the regulations and directions of supervisory authorities such as the European Central Bank, the European Banking Authority, and the Central Bank of Cyprus.

Depending on the service or product offered to you and/or the particular circumstances, the processing purposes may include evaluation of creditworthiness, verification controls for identity and age, fraud and money laundering prevention, fulfilment of obligations and the submission of reports deriving from tax laws, as well as the risk management within the Bank.

3.5 Processing of personal data of children

A child is defined as any person below the age of 18 years old. In those cases where personal data of children are to be processed, the Bank will proceed only after obtaining the explicit consent of the child's parents or legal guardians, unless otherwise permitted or required by law. The Bank does not provide online services to children. However, we may provide the child with view-only access to own accounts via myAncoria, our online banking venue, after proper application and consent by the child's parents or legal guardians.

4. Who receives your personal data?

Within Ancoria Bank

In the context of the Bank's operation, various Bank departments may receive your personal data. This is done in order for the Bank to carry out its contractual and legal obligations, as well as to be able to offer you better service.

Outside Ancoria Bank

The Bank may from time to time assign the processing of your personal data to third parties referred to as “Data Processors”. In such cases, the relevant information to be transmitted will be restricted to the minimum necessary and will only be used for specified and explicit purposes.

In addition, the Bank ensures that each Data Processor provides adequate assurances and that it processes your personal data in accordance with the GDPR (e.g. by signing confidentiality and data processing agreements).

Indicatively, and without limitation, the Bank’s Data Processors include:

- (i) companies managing technical support services (IT and Cloud Providers);
- (ii) companies/persons providing advisory services, for example accounting or law firms, financial and business consultants;
- (iii) companies involved in card payment management and processing, such as JCC Payment Systems Ltd, DIAS Interbanking Systems S.A., EveryPay Payment Services S.A., Marqeta Inc., and VISA Inc.;
- (iv) companies providing electronic signature solutions such as DocuSign France (with headquarters in the United States);
- (v) companies providing digital identity verification services such as Onfido SAS France;
- (vi) companies providing archiving services, as well as companies providing marketing services;
- (vii) companies managing non-performing loans;
- (viii) debt collection agencies.

In addition, and in order to comply with its legal and/or regulatory obligations, as well as to fulfil its contractual obligations towards you, the Bank may transfer your personal data to various government authorities or agencies and/or other organisations, such as:

- (i) The European Central Bank (ECB), the Central Bank of Cyprus (CBC), the Cyprus Securities and Exchange Commission (CySEC), and the European Investment Fund (EIF);
- (ii) Artemis Bank Information Systems Ltd, Bank Information Systems S.A. (Tiresias);
- (iii) MOKAS and other competent authorities, in the context of compliance with court orders or regulatory acts;
- (iv) Tax authorities, and/or other government departments/agencies for the purposes of state allowances provision and compliance with tax legal and regulatory framework;
- (v) Valuers, consultants, auditors;
- (vi) Correspondent banks such as the Bank of New York Mellon;
- (vii) Other financial institutions or similar organisations.

5. Retention of personal data

The Bank processes and stores your personal data for the duration of the contractual relationship with you, including the stage of discussions prior to the conclusion of a contract.

For existing customers

Upon expiration and/or termination of the contractual relationship with you, the Bank maintains and/or archives your personal data for up to 10 years in accordance with the relevant Directive of the Commissioner for the Protection of Personal Data.

It is clarified that the retention of your personal data may be extended in time, if deemed necessary in the framework of a tax investigation, court proceedings or any other investigation by an agency of the Republic of Cyprus or another supervisory authority.

For prospective customers

If you are a prospective customer, the Bank retains your personal data for a period of up to 6 months from the date you are notified of the rejection of your application or from the time, you withdraw your application for the provision of banking and/or financial services.

For more details on the above, please [click here](#) for the relevant circular by the Commissioner for the Protection of Personal Data.

6. Is personal data transferred to third countries or international organisations?

Your personal data is transferred to third countries (countries outside the European Economic Area - EEA), only in cases where it is necessary in order for the Bank to provide you with its services, or where it is necessary in order to carry out your instructions (e.g. payment orders, investment orders), or when you provide the Bank with your consent.

Furthermore, such transfer takes place when required by legislation (e.g. tax legislation, Foreign Account Tax Compliance Act (FATCA), Multilateral Competent Authority Agreement on Automatic Exchange of Financial Account Information (CRS)).

In any case, the Bank ensures that the organisation receiving your personal data provides the necessary safeguards and an adequate level of data protection in accordance with the GDPR.

7. Your data protection rights

You can exercise the following data protection rights under to the GDPR:

- (a) **right to access personal data:** Under this right, you may receive information which concerns you free of charge and/or obtain copies of your personal data held by the Bank.
- (b) **right to rectification of personal data:** Under this right, you may at any time request to correct or complete your personal data.
- (c) **right to erasure ("right to be forgotten"):** Under this right you can request the Bank to delete your personal data.

It is clarified that the Bank reserves its right to deny the said erasure, if the processing is necessary for the Bank to comply with its legal obligation, for reasons of public interest and/or for the exercise of its legal claims.

- (d) **right to restriction of processing of your personal data:** Under this right you may request the Bank to restrict the processing of your personal data if you contest its accuracy, the lawfulness of its processing and/or because it is not necessary for the processing purposes they had been collected for and/or when you have already objected to the Bank in processing your data in accordance with the **right to object** below and you expect the Bank's position as to the legitimate grounds which override your opposition.
- (e) **right to data portability:** Under this right, you may receive your personal data, in a structured, commonly used and machine-readable form, and to transfer it to other organisations/companies or ask the Bank to directly do so on your behalf.
- (f) **right to object:** You have the right to object to the processing of your personal data, including profiling, based on the legitimate and/or public interest when you deem that this is justified due to a particular situation that concerns you.

In such cases, the Bank shall no longer process your personal data unless it demonstrates compelling legitimate grounds for the processing which override your interests, rights and freedoms or if the processing serves the establishment, exercise or defence of legal claims.

You may object at any time to the processing of your personal data for purposes related to direct marketing, including profiling to the extent that it concerns direct marketing. In case the Bank processes your personal data for marketing purposes, any related processing shall cease.

- (g) **right to withdraw your consent:** as mentioned in section 3.3 above, you reserve the right at any time to withdraw your consent to collection and processing of your personal data. In such

case, the withdrawal of the consent does not affect the legality of the data processed prior to the revocation.

It is noted that the abovementioned rights apply with the restrictions provided for under the GDPR. If you wish to exercise any of the above rights or for any questions regarding the processing of your personal data, you may contact the Banking Centre you collaborate with, the Bank's Customer Service Centre, the Bank's Data Protection Officer (dpo@ancoriabank.com) or fill out the relevant form through the Bank's website (www.ancoriabank.com).

8. How can you file a complaint?

In case you have any complaint and/or dispute in regard to the way your personal data is processed, you are kindly requested to notify the Bank through the aforementioned communication channels and the Bank will immediately undertake to investigate and inform you in regard to your complaint.

In addition, you are entitled to submit a complaint to the Commissioner for Personal Data Protection of the Republic of Cyprus. You can find information regarding the filing of complaints on the website of the Office of the Commissioner (www.dataprotection.gov.cy) or to other relevant authorities of your country of residence.

9. Are you obligated to provide personal data?

In order for the Bank to establish a business relationship with you, you will have to provide the Bank with your personal data to the extent that it is necessary for the execution and conclusion of this business relationship and for the fulfilment of the contractual obligations accompanying it.

Additionally, the Bank is obliged under the "Prevention and Suppression of Money Laundering Activities" Law (N. 188(I)/2007) to verify the identity of its clients and/or establish the purpose and nature of transactional behaviour, and is therefore required to receive all necessary data/documents in order to be able to conclude a business relationship with you personally or in any other capacity as referred to in the preface of this Notice, e.g. as a company's director and/or provide any banking services and/or execute any transactions.

Without this data and documentation, the Bank will not be able to establish a business relationship with you or it may no longer be able to execute an existing contract and will have to terminate it.

10. Does automated decision-making take place?

Automated individual decision-making means the process of making decisions through automated means of processing personal data/details, without human intervention, e.g. automated approval/refusal of an application for a credit facility. Unless there is absolutely no other way, automated individual decision-making is not mandatory and you can always request a manual decision-making process instead.

The Bank may employ automated decision-making insofar as this is authorised by legislation, or if you have provided an explicit consent, or if it is necessary for the performance of a contract. In any such case, you will always be adequately informed in advance on the specifics of automated decision-making and you can always express your opinion, contest the said automated decision, and request human assessment and intervention from our side.

11. Is your data used for profiling?

Profiling refers to the automated processing of your personal data for the evaluation of certain personal aspects that concern you.

In compliance with the "Prevention and Suppression of Money Laundering Activities" Law (N. 188(I)/2007), and the relevant regulations of competent authorities as amended from time to time, the Bank may, among other reasons, use profiling while processing your payment transactions. Such measures are also useful for your own protection.

Furthermore, the Bank may employ profiling as part of the evaluation of your creditworthiness i.e. whether you will be able to meet the contractual obligations you undertake. This measure is designed to achieve proper lending, under the Bank's risk management framework, in compliance with the relevant Central Bank of Cyprus Directives on Credit Granting and Review Processes.

Finally, profiling may also be employed in order for the Bank to be able to identify whether a particular product is deemed appropriate for your interests, objectives, characteristics and benefit, in compliance with the relevant European Banking Authority Guidelines, 2015/18, on product oversight and governance arrangements for retail banking products.

12. Information security

The Bank implements a range of controls in order to ensure and maintain the confidentiality, integrity, and availability of your personal data. These measures cover physical and environmental security, the security of the Bank's network, technical infrastructure and information systems, as well as the organisational aspects of information security. Any Bank personnel and any third party who carries out any personal data processing on behalf of the Bank is required to follow strict compliance standards and is obligated to protect personal data and apply appropriate measures for the use and transfer of such data.

13. Privacy notice for electronic channels

For an overview of how the Bank processes and protects personal data via its electronic channels, please [click here](#).

14. Changes / amendments to the Privacy Notice

The Bank reserves the right to amend this Notice from time to time by informing you accordingly.

In any case, you are invited to periodically visit the Bank's website (www.ancoriabank.com) for information on the updated edition of the Notice and/or for any other useful information.

Do not hesitate to contact us via the Bank's Data Protection Officer for anything you may need regarding the present Notice and/or for other issues related to data protection.